(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年8 月4 日 (04.08.2005)

PCT

(10) 国際公開番号
WO 2005/071640 A1

(51) 国際特許分類[7]: G09C 1/00

(21) 国際出願番号: PCT/JP2005/001437

(22) 国際出願日: 2005 年1 月26 日 (26.01.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-016881 2004 年1 月26 日 (26.01.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 古川 潤 (FURUKAWA, Jun) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP). 寺西 勇 (TERANISHI, Isamu) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP).

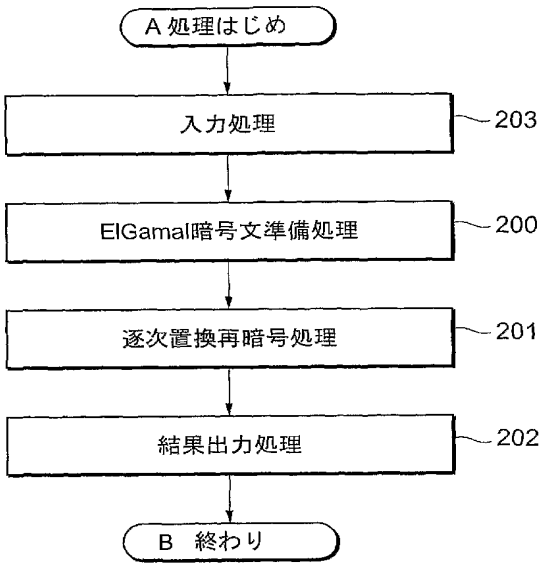
(74) 代理人: 池田 憲保 (IKEDA, Noriyasu); 〒1050003 東京都港区西新橋一丁目４番１０号 第３森ビル Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS,

[続葉有]

(54) Title: METHOD AND DEVICE FOR CALCULATING A FUNCTION FROM A PLENTY OF INPUTS

(54) 発明の名称: 多数の入力から関数を計算する方法および装置



A PROCESS START
203 INPUT PROCESS
200 E|Gama| ENCRYPTED SENTENCE PREPARATION PROCESS
201 SUCCESSIVE REPLACEMENT RE-ENCRYPTION PROCESS
202 RESULT OUTPUT PROCESS
B END

(57) Abstract: In an input process, a circuit and an input bit to the circuit are inputted to a plurality of computers. Firstly, one of the computers performs calculation and transmits the calculation result to another computer. Next, the another computer which has received the calculation result performs the next calculation. Thus, calculation is performed by one computer after another. When all the computers have performed calculation once, the last computer which has performed calculation transmits the calculation result to the first computer which has performed calculation. After this, calculation is performed by one computer after another and the calculation result is transmitted to the next computer, thereby repeating the calculation of each cycle. Thus, it is possible to realize calculation of a value of a given function by using a device including a plurality of computers, with a more simple configuration.

(57) 要約: 入力処理では、複数の計算装置に、回路と、回路への入力ビットとが入力され、まず一台の計算装置が計算を行い、その計算結果を他の計算装置のうち一台に送り、次にその計算結果を受け取った前記計算装置がその次の計算を行う、というとように一台ずつ順に計算を行ってその計算結果を次の一台に回し、全ての計算装置が一度ずつ計算が終わったら、最後に計算をした計算装置が最初に計算をした計算装置に計算結果を送り、以後何度も、一台ずつ順に計算を行ってその計算結果を次の一台に回すという各周の計算を繰り返す事を特徴とする。これにより、複数の計算装置を含む機器を用いて与えられた関数の値を計算することをより簡単な構成で実現する。

WO 2005/071640 A1

LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書
— 請求の範囲の補正の期限前の公開であり、補正書受領 の際には再公開される。

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

多数の入力から関数を計算する方法および装置

発明の背景

本発明は、与えられた関数の入力が複数の装置に分散されて保持されている時に、これら装置が連動してこの関数の出力を計算する方法に関し、特に各装置が他の装置と行う通信回数が与えられた関数に依らず定数回で計算できる方法およびシステムに関する。

背景技術

与えられた関数の入力が複数の装置に分散されて保持されている時に、これら装置が連動してこの関数の出力を計算する方法の従来の技術として、 Beaver、Micali、Rogaway が文献「D. Beaver、S. Micali、and P. Rogaway、『The round complexity of secure protocols』、Annual ACM Symposium on Theory of Computing 22、ページ 503-513、1990 年」にて提案した方法がある。以降この文献を非特許文献 1 と呼ぶ。

非特許文献 1 に開示される技術は、ネットワークで繋がる λ 人の計算者 u_α がそれぞれ秘密の入力 x_α を持ち、任意の関数 g が与えられたときに、計算者が互いに協力して関数の出力 $g(x_1, \ldots, \lambda)$を計算する方法で、各計算者の秘密が $g(x_1, \ldots, x_\lambda)$ 以上に漏ることがなく、かつ、この計算に必要な通信回数が定数となる方法である。非特許文献1に開示される技術について図1、図２および図１９を用いて説明する。

[ガードブル回路]

[記法]

回路 f は m 個の論理ゲートで構成されるものとし、各ゲートを $G_1,\ldots,G_l,\ldots,G_m$ とする。各ゲート図１９に示されるように、２入力１出力で、各出力は複数のゲートに入力されても良いものとする。G_k の出力配線は一般に複数のゲートに入力されるが、配線を流れる信号の値はどれも同じ値で０または１とする。また、このゲート G_k から出る配線を全て w_k と呼ぶ。回路 f に入力される配線の本数を n 個とし、これを

{wk} k = m+1, ..., m+n とする。$w_1,...,w_l$ を回路 f の出力とする。

計算者の人数を λ、計算者の集合を

$$\left\{u^{(\alpha)}\right\}_{\alpha=1, ..., \lambda}$$ とする。

$u^{(\alpha)}$ が回路 f へ入力するビットの個数を l_α 個とし、それらの和を n とする

$$(\Sigma_{\alpha=1}^{\lambda} l_\alpha = \lambda). \quad k = m+1, ..., m+n$$

に関して各 w_k に入力されるビットを b_k とし、それぞれのビットを $u^{(\alpha)}$ に l_α 個ずつ次のように割り振る。すなわち、$u^{(\alpha)}$ は集合

$$\{b_k \in \{0,1\}\}k = m + \Sigma_{\beta=1}^{\alpha-1} l_\beta + 1, ..., m + \Sigma_{\beta=1}^{\alpha} l_\beta$$

を決定する。

ゲート G_k にゲート G_i とゲート G_j の出力が入力されたとき、G_j の出力 b_j、G_j の出力 b_j、と G_k の出力 b_k の間の関係を、

$$b_k = b_i ◎_{G[k]} b_j$$

と表す。また、口は bit の排他的論理和、・は文字列の連結を表すとする。

t は安全変数で、G, H, F は tλ ビットの文字列を出力する疑似乱数生成器とする。

[構成]

プロトコルは大きく三つの処理、(1) 入力処理 402、(2) 多人数計算によるガーブルド回路の並列構築処理 400 と、(3) 入力の開示と回路の計算を行う結果出力処理 401 とに分かれる。

入力処理 402 は次の様に行う。計算する回路に関する情報、他の計算者に関する情報、各装置の入力データを、各装置に入力する。

ガーブルド回路の並列構築処理 400 は次の様に行う。この処理の過程では、図 2 に示される、λ 個の計算装置 501 が個別に計算を行うフェーズ 502 と、全ての計算機が互いに通信するフェーズ 503 が交互に繰り返し行われる。そして、この繰り返しの回数としてある定数回 504 が存在して、計算したい関数がどのようなものであれ以下の処理は終了できる。また、各通信フェーズでは、各計算装置がその他の全ての計算装置にデータを送信するが、この時送信するデータを生成するために、この送信と同じ通信フェーズで行われる他の計算装置の送信データを必要とし

てはならない。すなわち、他の計算装置のデータを待たねばできない送信があるとき、この送信を行う通信フェーズを、データを待っている通信フェーズとは別のものと数える。

[1] 計算者は協力してtビットの文字列の集合

$$\{s^{\alpha}_{k'}s^{\alpha}_{k} \in R\{0,1\}^{t}\}\ k=1, \ldots, m+n;\ \alpha=1, \ldots, \lambda$$

及びビットの集合

$\{\rho_k \in R\{0,1\}\}$

を一様無作為に、計算者全員に秘密分散される様に生成する。ここで、

$S_k := s_k^1 \cdot s_k^2 \cdot \ldots s_k^{\lambda}$

$S'_k := s'^1_k \cdot s'^2_k \cdot \ldots s'^{\lambda}_k$ とする。$\{S_k\},\{\rho_k\}$は$\lambda_k \square b_k = 0$であるならば、回路の計算フェーズにおいて$S_k$が公開され、$\lambda_k \square b_k = 1$ならば$S'_k$が公開されることになる。

[2] それぞれの計算者

u_αには、

$$\{s^{\alpha}_{k}\}\ k=1, \ldots, m+n$$

が明かされる。

[3] それぞれの計算者

u_αは、k=1, ..., m+n に関して、それぞれ$t\lambda$ビットの文字列である

$$g^{\alpha}_{k} = G(s^{\alpha}_{k})$$
$$g'^{\alpha}_{k} = G(s'^{\alpha}_{k})$$
$$h^{\alpha}_{k} = H(s^{\alpha}_{k})$$
$$h'^{\alpha}_{k} = H(s'^{\alpha}_{k})$$
$$f^{\alpha}_{k} = F(s^{\alpha}_{k})$$
$$f'^{\alpha}_{k} = F(s'^{\alpha}_{k})$$

を計算し、

$$\{g^{\alpha}_{k'}, g'^{\alpha}_{k'}, h^{\alpha}_{k'}, h'^{\alpha}_{k'}, f^{\alpha}_{k'}, f'^{\alpha}_{k'}\}_k$$

をコミットし、さらにこれらの値を正しく計算したことを他の計算者に証明する。

[4] k = m+1, ..., m+n に関して、計算者達は、

$\sigma_k^1 \cdot \ldots \sigma_k^\lambda = S_k$ もし $\lambda_k \square b_k = 0$

$\sigma_k^1 \cdot \ldots \sigma_k^\lambda = S'_k$ もし $\lambda_k \square b_k = 1$

を秘密に分散して計算する。

[5] 計算者達は協力して k=1, ..., m+n に関して、

$A_k = g_i^1 \square \ldots \square g_i^\lambda \ \square g_j^1 \square \ldots \square g_j^\lambda \ \square S_k$ もし $\rho_i \circledcirc_{G[k]} \rho_j = \rho_k$

$A_k = g_i^1 \square \ldots \square g_i^\lambda \ \square g_j^1 \square \ldots \square g_j^\lambda \ \square S'_k$ もし $\rho_i \circledcirc_{G[k]} \rho_j \neq \rho_k$

$B_k = h_i^1 \square \ldots \square h_i^\lambda \ \square g'^1_j \square \ldots \square g'^\lambda_j \ \square S_k$ もし $\rho_i \circledcirc_{G[k]} \rho_j = \rho_k$

$B_k = h_i^1 \square \ldots \square h_i^\lambda \ \square g'^1_j \square \ldots \square g'^\lambda_j \ \square S'_k$ もし $\rho_i \circledcirc_{G[k]} \rho'_j \neq \rho_k$

$C_k = g'^1_i \square \ldots \square g'^\lambda_i \ \square h_j^1 \square \ldots \square h_j^\lambda \ \square S_k$ もし $\rho'_i \circledcirc_{G[k]} \rho_j = \rho_k$

$C_k = g'^1_i \square \ldots \square g'^\lambda_i \ \square h_j^1 \square \ldots \square h_j^\lambda \ \square S'_k$ もし $\rho'_i \circledcirc_{G[k]} \rho_j \neq \rho_k$

$D_k = h'^1_i \square \ldots \square h'^\lambda_i \ \square g'^1_j \square \ldots \square g'^\lambda_j \ \square S_k$ もし $\rho'_i \circledcirc_{G[k]} \rho'_j = \rho_k$

$D_k = h'^1_i \square \ldots \square h'^\lambda_i \ \square g'^1_j \square \ldots \square g'^\lambda_j \ \square S'_k$ もし $\rho'_i \circledcirc_{G[k]} \rho'_j \neq \rho_k$

を秘密に分散して計算する。但しゲート G_k に入力される信号はゲート G_i とゲート G_j の出力とする。この様子を図１９に示す。結果出力処理 401 における入力の開示と回路の生成は次の様に行う。

[1] 計算者は

$\{\rho_k\}$ k=1, ..., l

$\{f_k^\alpha\}$ k=1, ..., m+n; α=1, ..., λ

$\{\sigma_k^1 \cdot \ldots \cdot \sigma_k^\lambda\}$ k=1, ..., m+n

$\{A_k, B_k, C_k, D_k\}\}$ k=1, ..., m+n

を公開する。

[2] 回路の入力により近い k から順番に k=1, ..., m+n に関して、S_i または S'_i、及び S_j、または、S'_j から、次のようにして S^*_k を得る。これは S_k または S'_k である。

$S_k^* = A_k \square g_i^1 \square \ldots \square g_i^\lambda \ \square g_j^1 \square \ldots \square g_j^\lambda$ もしS_i, S_jを持っているなら

$S_k^* = B_k \square h_i^1 \square \ldots \square h_i^\lambda \ \square g'_j{}^1 \square \ldots \square g'_j{}^\lambda$ もしS_i, S'_jを持っているなら

$S_k^* = C_k \square g'_i{}^1 \square \ldots \square g'_i{}^\lambda \ \square h_j^1 \square \ldots \square h_j^\lambda$ もしS'_i, S'_jを持っているなら

$S_k^* = D_k \square h'_i{}^1 \square \ldots \square h'_i{}^\lambda \ \square g'_j{}^1 \square \ldots \square g'_j{}^\lambda$ もしS'_i, S'_jを持っているなら

[3] 全ての $\alpha=1, \ldots, \lambda$; $k=1, \ldots, m+n$ に関して

$f^\alpha{}_k = F(s^\alpha{}_k)$、

$f'^\alpha{}_k = F(s'^\alpha{}_k)$

を確認することで、$S^*{}_k = S_k$ または $S^*{}_k = S'_k$ を確認する。

[4] 全ての計算者は $k=1, \ldots, l$ に関して、S_k を手にいれた場合は $\rho_k + b_k = 0$、S'_k を手にいれた場合は $\rho_k + b_k = 1$ が成り立つことより、b_k を求める。

技術分野の欄に記述された様な方法のその他の従来の技術として、Ishai、Kushilevitz は、文献「Y. Ishai and E. Kushilevitz、『Randomizing Polynomials: A new Representation with Applications to Round-Efficient Secure Computation』、IEEE Symposium on Foundations of Computer Science 2000、ページ 294-304」にて提案した方法がある。以降この文献を非特許文献２と呼ぶ。非特許文献２の従来の技術を図３および図４を用いて説明する。

［ランダマイジング多項式］

非特許文献２には、与えられた関数をある有限体上の低い次数の多項式で表現する方法が提案されている。特に任意の関数が次数３の多項式で表現可能であることが示されている。次数が低い多項式を評価することは定数回のラウンドで可能である。一般に関数は、回路等様々な形で表現することができる。

次にあげるブランチング問題も一般の関数を表現することができる。ブランチング問題 BP = (G,φ、s,t) を mod-p ブランチング問題と呼ぶ。G = (V, E) は向き付けられたグラフ、φ はラベル付け関数で、G のそれぞれの辺に、1、$x^1{}_i$、あるいはその否定 $x^0{}_i$ のいずれかを関係付けるもの、s, t は特別な頂点である。

入力 $x = (x_1, \ldots, x_n)$が与えられたとき、ラベル付け関数 φ により G の部分グラフ Gx が与えられる。BP で計算される boolean 関数 f の値は、G_x における s-t を結ぶ経路の数を p で割った余りが 0 ならば f(x) = 0、そうでなければ f(x) = 1 とする。

BP の大きさを G の頂点の数とする。

BP の大きさを l とする。部分グラフ Gx の l¥timesl 隣接行列を Hx とすると、s-t 間を結ぶ経路の数は、

$$(I+H_x + H_x^2+ \cdot s)_{st} = ((1-H_x)^{-1})_{st} \bmod p$$

$$= \det M_x / \det (I-H_x) \} \bmod p$$

となる。ここで M_x は行列 (I-Hx) から s 行と t 列を除いた行列とする。よって、

$$f(x) = 0 \Leftrightarrow \mathrm{rank}\ (M_x) = I-1$$

$$f(x) = 0 \Leftrightarrow \mathrm{rank}\ (M_x) = I$$

となる。また、M_x は x に関して高々 1 次の成分からなる。

[計算方法]

ブール関数 f が与えられ、その入力 x が複数の計算者に分配されている時に、ランダマイジング多項式の方法を用いて f(x)を求める方法を記す。

【００７９】

図３に示すように、

[1] 計算する関数に関する情報、他の計算者に関する情報、各装置の入力データを、各装置に入力する（605）。

[2] f に対応する BP を構成する（600）。

[3] 次の処理を十分な回数並列して行う（601）。

[処理]

図４に示すように、

全ての計算者は各成分を分散して lxl 行列 R_1, R_2 を一様無作為に生成し（603）、3 行列 R_1, M_x, R_2 の積である $R_1M_xR_2$ を計算する（604）。

各成分は R_1, R_2, x の要素の高々３次の式であり、その計算に必要なラウンド数は高々定数回である。

[4] 全ての rank$R_1M_xR_2$ の値から M_x の rank が I であるかを推測し、I である確率が高ければ 1 を、でなければ 0 を出力する（602）。

上記方法において、rank (M_x) = rank (M'_x)であれば、$R_1M_xR_2$ と $R_1M'_xR_2$ の分布は同じになるので、x に関する情報は f(x) 以外は新たに漏ることはない。

さらに、いかなる I に対しても、rank (Mx) = I であるならば rank $(R_1M_xR_2)$ = I と

なる確率は 0.08 より大きいため、項目２の処理を実行する回数は l に依存しない。

[計算量と通信量]

ガーブルド回路を用いた方法では、各ゲートに関する計算は独立して行われ、全体の通信量と計算量はゲートの数に比例する。t-n 閾値分散($2t^2$ に比例する。t-n 閾値分散での計算とは n 人で秘密を分散して計算を行うが、このうち t 人が各自知っているデータを持ち寄らない限り、分散された秘密や計算の途中の意味のあるデータを知ることができない計算方法である。

ランダマイジング多項式を用いた方法では、t-n 閾値分散が行われた場合で、t^2 と BP の大きさの２乗に比例し、ラウンド数は 2(3)となる。

ランダマイジング多項式の方法では通信量と計算量はゲート数の高々１次に比例する。さらに、最高次の係数はランダマイジング多項式の方法のものが断然低く、効率的である。

しかし、ここでは t-n 閾値分散で $t > n/2$ である様な場合で第三者が計算の正当性を検証できることを要求する場合に特に注目する。この様な場合に前述の方法を拡張することは容自明である。拡張の結果は、ガーブルド回路を用いた方法で全体の通信量と計算量はゲートの数と t3 に比例し、ランダマイジング多項式の方法を用いた場合、通信量と計算量がゲート数の 1.5 乗に比例し、ゲート数が大きい場合効率的ではない。

第１の問題点は、非特許文献１の方法は、各計算者の計算量及び計算の正当性を検証する検証者の計算量が膨大になるということである。

その理由は、各計算者は疑似乱数生成装置の出力を計算しなければならないが、この計算を正しく行ったことを計算結果を隠したまま証明する必要があるためである。

第２の問題点は、非特許文献２の方法も、やはり各計算者の計算量及び計算の正当性を検証する検証者の計算量が膨大になるということである。

その理由は、各計算者が計算する計算量が、関数を回路で表現した場合のゲート数の 1.5 乗に比例し、かつ多くの場合ゲート数は非常に多いため、全体の計算量が膨大になると言うことである。

発明の開示

本発明の目的は、回路を表現するゲート数が多くなってもその計算装置がゲート数に比例するに留め、計算装置がその計算の正当性を証明すべき疑似乱数生成装置の出力を計算する必要がなく、かつ計算装置の通信回数が関数に依らずに定数回となる計算方法およびシステムを提供することにある。

本発明の計算方法は、複数の計算装置を含む機器を用いて与えられた関数の値を計算する方法であって、

入力処理と、

出力処理とからなり、

前記入力処理では、前記複数の計算装置に、回路と、前記回路への入力ビットとが入力され、

まず一台の前記計算装置が計算を行い、その計算結果を他の前記計算装置のうち一台に送り、次にその計算結果を受け取った前記前記計算装置がその次の計算を行う、というとように一台ずつ順に計算を行ってその計算結果を次の一台に回し、全ての前記計算装置が一度ずつ計算が終わったら、最後に計算をした計算装置が最初に計算をした計算装置に計算結果を送り、以後何度も、一台ずつ順に計算を行ってその計算結果を次の一台に回すという各周の計算を繰り返す事を特徴とする。

本発明の他の形態による計算方法は、複数の計算装置を含む機器を用いて与えられた関数の値を計算する方法であって、

入力処理と、

ElGamal 暗号文準備処理と、

逐次置換再暗号処理と、

結果出力処理とからなり、

前記入力処理は、

前記複数の計算装置に複数のゲートから構成された回路の情報及び前記複数の計算装置に関する情報が入力される、情報入力ステップと、関数の入力データを複数に計算装置の個数に分散したデータである複数の部分データを、それぞれの計算装置にそれぞれ一つずつ入力する分散入力ステップと、からなり、

前記 ElGamal 暗号文準備処理は、少なくとも一つの計算装置が、与えられた関

数を実現する回路のゲートに対応した ElGamal 暗号文の集合を生成する ElGamal 暗号文準備ステップとからなり、

前記逐次置換再暗号処理は、

置換再暗号処理を各計算装置が順番に行う処理で、前記置換再暗号処理は、順番が回ってきた計算装置が、一つ前の順番に対応する計算装置から ElGamal 暗号文の集合を受け取る暗号文取得ステップと、

前記暗号文取得ステップにて受け取った暗号文の集合を順序を入れ替えて置換し、それらを再暗号化する暗号文の置換と再暗号化ステップと、

前記暗号文の置換と再暗号化ステップで生成したデータを、少なくとも次の順番の計算装置に公開するステップと、からなり、

前記結果出力処理は、

前記逐次置換再暗号処理で生成された暗号文の一部を復号あるいは部分復号する部分復号ステップと、

前記前記逐次置換再暗号処理で生成された暗号文の中で前記回路の入力に対応するデータを暗号化している暗号文を復号する復号ステップと、

前記復号ステップで復号されたデータと、前記部分復号ステップで部分復号されたデータを用いて、回路の出力を評価する回路の評価ステップと、からなることを特徴とする。

この場合、前記各ゲートに対応する ElGamal 暗号文の集合は、前記各計算装置が各ゲートに対応して生成した秘密鍵の ElGamal 暗号文の集合であり、

前記 ElGamal 暗号文を生成するのに用いた公開鍵は、このゲートに入力される二つの信号を生成するゲートに対応する公開鍵の和であることとしてもよい。

また、前記入力処理として、各計算装置に ElGamal 暗号方式の領域変数を入力するステップが行なわれ、

前記 ElGamal 暗号文準備処理として、各前記計算装置が、各前記回路の各ゲートに対応して、ElGamal 暗号文の秘密鍵を生成するゲート秘密鍵生成ステップが行なわれ、

各計算装置では、

前記ゲート秘密鍵の生成ステップにて生成した秘密鍵に対応するゲート公開鍵

を生成するゲート公開鍵の生成ステップと、

前記ゲート公開鍵の生成ステップにて生成した公開鍵の正当性の証明を生成するゲート公開鍵の正当性の証明生成ステップと、

前記ゲート公開鍵の正当性の証明生成ステップにて生成したゲート公開鍵の正当性の証明を公開するゲート公開鍵の正当性の証明公開ステップと、

各前記回路のゲートで回路への入力が直接入力されるゲートに対応して、ElGamal 暗号文の秘密鍵を生成する入力のゲート秘密鍵の生成ステップと、

前記入力ゲート秘密鍵の生成ステップにて生成した秘密鍵に対応する入力ゲート公開鍵を生成する入力のゲート公開鍵の生成ステップと、

前記入力のゲート公開鍵の生成ステップにて生成した公開鍵の正当性の証明を生成する入力のゲート公開鍵の正当性の証明生成ステップと、

前記入力のゲート公開鍵の正当性の証明生成ステップにて生成し入力の公開鍵の正当性の証明を公開する入力のゲート公開鍵の正当性の証明公開ステップと、

その他の各計算装置が生成して公開したゲート公開鍵を取得するゲート公開鍵取得ステップと、

前記ゲート公開鍵取得ステップにおいて取得したゲート公開鍵を統合するゲート公開鍵の統合ステップと、

前記ゲート公開鍵の統合ステップにおいて統合したゲート公開鍵により、この計算装置が生成したゲート秘密鍵を暗号化するゲート秘密鍵の暗号化ステップと、

前記ゲート秘密鍵の暗号化ステップにおいて生成したゲート秘密鍵の暗号文を公開するゲート秘密鍵の暗号文の公開ステップと、

前記ゲート秘密鍵の暗号文の正当性証明を生成するゲート秘密鍵の暗号文の正当性の証明生成ステップと、

前記ゲート秘密鍵の暗号文の正当性の証明生成ステップにおいて生成したゲート秘密鍵の暗号文の正当性の証明を公開するゲート秘密鍵の暗号文の正当性の証明公開ステップと、

各計算装置に入力された回路の入力の部分に対応する暗号文を生成する入力の暗号文生成ステップと、

前記入力の暗号文生成ステップにて生成した回路の入力の部分に対応する暗号

文の正当性の証明を生成する入力の暗号文の正当性の証明生成ステップと、

前記入力の暗号文の正当性の証明生成ステップにおいて生成した証明を公開する入力の暗号文の正当性の証明公開ステップと、

出力のゲートに対応する暗号文を生成して公開する出力の暗号文の生成ステップと、を含み、

前記置換再暗号処理が、

前記ゲート秘密鍵の暗号文の集合の順番をあらかじめ決められた許された置換の方法から無作為に一つの置換を選んで入れ替えて再暗号化するゲート秘密鍵の暗号文の置換と再暗号化ステップと、

前記入力の暗号文の集合の順番をあらかじめ決められた許された置換の方法から無作為に一つの置換を選んで入れ替えて再暗号化する入力の暗号文の置換と再暗号化ステップと、

前記出力の暗号文の集合の順番をあらかじめ決められた許された置換方法から無作為に一つの置換を選んで入れ替えて再暗号化する出力の暗号文の置換と再暗号化ステップと、

前記ゲート秘密鍵の暗号文の置換と再暗号化ステップと入力の暗号文の置換と再暗号化ステップと出力の暗号文の置換と再暗号化ステップとにおいてなされた置換と再暗号化の正当性の証明を生成し公開するゲート秘密鍵の暗号文と入力の暗号文と出力の暗号文の置換と再暗号化の正当性の証明生成と公開ステップと、を含み、

前記結果出力処理の部分復号ステップが、

前記計算装置が互いに通信及び計算することで前記ゲート秘密鍵の暗号文を部分復号するゲート秘密鍵の部分復号ステップと、

前記計算装置が互いに通信及び計算することで前記入力の暗号文を部分復号する入力の暗号文の部分復号ステップと、

前記計算装置が互いに通信及び計算することで前記出力の暗号文を部分復号する出力の暗号文の部分復号ステップと、

前記ゲート秘密鍵の部分復号ステップと入力の暗号文の部分復号ステップと出力の暗号文の部分復号ステップとでなされた部分復号の正当性の証明を生成し公

開するゲート秘密鍵と入力の暗号文と出力の暗号文の部分復号ステップの正当性の証明生成と公開ステップと、を含み、

他の計算装置の公開した種々の正当性の証明を検証するステップを含む、こととしてもよい。

本発明の計算システムは、複数の計算装置と、

複数の計算装置と通信する手段と、

入力処理手段と、

ElGamal 暗号文準備手段と、

置換再暗号処理手段と、

結果出力処理手段と、からなる関数を評価する計算システムであって、

前記入力処理手段は、出力を求めたい回路の情報と、前記複数の計算装置に関する情報と、前記複数の計算装置がそれぞれ前記回路の入力のどの部分を所持しているかという情報と、を入力し、

前記 ElGamal 暗号文準備処理手段は、与えられた関数を実現する回路のゲートに対応した ElGamal 暗号文の集合を生成する ElGamal 暗号文を準備し、

前記置換再暗号処理手段は、

順番が回ってきた計算装置が、一つ前の順番に対応する計算装置から ElGamal 暗号文の集合を受け取る暗号文取得手段と、

前記暗号文取得手段により受け取られた暗号文の集合の順序を入れ替えて置換し、それらを再暗号化する暗号文の置換と再暗号化手段と、

前記暗号文の置換と再暗号化手段を用いて生成したデータを、少なくとも次の順番の計算装置に公開する手段と、からなり、

前記結果出力手段は、

置換再暗号処理手段で生成された暗号文の一部を復号あるいは部分復号する部分復号手段と、

前記前記逐次置換再暗号処理で生成された暗号文の中で前記回路の入力に対応するデータを暗号化している暗号文の自分に関する暗号化を復号する復号手段と、

前記複数の計算機が前記復号手段で復号したデータと前記複数の計算機が前記部分復号手段で部分復号されたデータを用いて回路の出力を評価する回路の評価

手段と、からなることを特徴とする。

本発明の他の形態による計算システムは、複数の計算装置、入力手段、出力手段を含み、まず一台の前記計算装置が計算を行い、その計算結果を他の前記計算装置のうち一台に送り、次にその計算結果を受け取った前記前記計算装置がその次の計算を行う、というとように一台ずつ順に計算を行ってその計算結果を次の一台に回し、全ての前記計算装置が一度ずつ計算が終わったら、最後に計算をした計算装置が最初に計算をした計算装置に計算結果を送り、以後何度も、一台ずつ順に計算を行ってその計算結果を次の一台に回すという各周の計算を繰り返す計算システムであって、

前記入力手段では前記計算装置に回路の情報と、前記回路への入力ビットの一部とが入力され、

第ゼロ周目の計算は第一の計算装置が第一周目の計算を行う前に行い、

前記複数の計算装置には、

前記各周の計算に使用される送られてきたデータを取得するデータ取得手段と、正当性証明検証手段と、署名文検証手段と、第一の計算装置のみが行う第一計算装置特別計算手段と、乱数生成を行う乱数生成手段と、本計算を行う本計算計算手段と、本計算で行った計算の正当性を証明する正当性証明作成手段と、署名手段とデータ送信手段とからなり、

前記送られてきたデータは、別の計算装置から送られてきたデータと、データ本体と、データ本体に対する正当性証明と、署名文とからなり、

前記署名文は、前記別の計算装置から送られてきたデータと、前記データ本体と、前記データ本体に対する正当性証明との組に対する署名文であるようなデータで、

前記正当性証明検証手段は前記送られてきたデータ中の正当性証明を検証し、

前記署名検証手段は、前記送られてきたデータ中署名文を検証し、

前記本計算は前記乱数生成手段で生成された乱数を用いて計算し、

前記署名手段が、前記送られてきたデータと、前記本計算で計算された計算結果であるデータ本体と、前記正当性証明作成手段で作成された正当性証明との組に対する署名文を作成し、

前記データ送信手段が、前記送られてきたデータと、前記本計算で計算された計

算結果であるデータ本体と、前記正当性証明作成手段で作成された正当性証明と前記署名手段で作成された署名文との組を送信する事を特徴とする。

この場合、前記送られてきたデータのデータ本体と前記本計算で計算されたデータ本体とが、第一周目の計算では、共に真理値群環上の多重配列エルガマル暗号文達と真理値群環上の拡張多重配列エルガマル暗号文達とからなる組であるとしてもよい。

また、各周の計算が、第一周目の計算手段と、第一周目以降の周の計算手段とからなり、

前記計算手段は、第ゼロ周目の計算手段では真理値群環上の多重配列エルガマル暗号文達と真理値群環上の拡張多重配列エルガマル暗号文達とからなる組を作成し、前記第一周目の計算手段が再暗号に使用する為の公開鍵を作成する再暗号用公開鍵作成手段と、送られてきたデータを変換するデータ変換手段と、秘密鍵変換手段と、乱数変換手段とからなり、

前記データ変換手段が、前記データ本体である暗号文の組を、真理値群環上の多重配列エルガマル暗号文達と真理値群環上の拡張多重配列エルガマル暗号文達とからなる別の組に変換する為の手段であり、

前記秘密鍵変換手段が、前記データ変換手段の計算結果である暗号文達の組に使用されている秘密鍵を再暗号用公開鍵作成手段で作成された公開鍵に対応する秘密鍵に変換する手段であり、

前記秘密鍵変換手段の計算結果が真理値群環上の多重配列エルガマル暗号文達と真理値群環上の拡張多重配列エルガマル暗号文達とからなる組であり、

前記乱数変換手段が前記データ変換手段の計算結果である暗号文達の組に使用されている乱数を変換する手段であり、

前記乱数変換手段の計算結果が真理値群環上の多重配列エルガマル暗号文達と真理値群環上の拡張多重配列エルガマル暗号文達とからなる組であるとしてもよい。

また、第一周目以降の周の計算手段が、第二周目の計算手段と第二周目以降の計算手段とからなり、

前記送られてきたデータのデータ本体と前記本計算で計算されたデータ本体と

が、第二周目の計算では、共に真理値群環上の多重配列エルガマル暗号文達と真理値群環上の拡張多重配列エルガマル暗号文達とからなる組であり、

前記第二周目の計算手段が、

前記送られてきたデータの前記データ本体を変換してエルガマル暗号文もしくは楕円曲線エルガマル暗号文を作成する暗号変換手段と、前記送られてきたデータのデータ本体の暗号文達を部分復号する部分復号手段とからなるとしてもよい。

さらに、第二周目以降の計算手段が、第三周目の計算手段のみからなり、第三周目の計算手段の前記本計算手段が、前記送られてきたデータをそのまま出力し、

前記正当性証明作成手段が空列を出力するとしてもよい。

本発明の多数の入力から関数を計算する方法は、ElGamal 暗号方式を利用して、その値を隠したゲートの入出力の対応表を生成する手段とを備え、各入力を持った装置が次々と順番に、図５に示すように ElGamal 暗号文の集合からなる対応表の順番を入れ替えるよう動作する。このような構成を採用し、各装置に分配された入力に対する関数の出力を計算することにより本発明の目的を達成することができる。

発明の効果

第１の効果は、各計算装置の計算量と通信量が回路のゲート数に比例するに留まり、効率的であることにある。

その理由は、各ゲート毎にゲートの入出力の対応表を ElGamal 暗号文で生成し、疑似乱数生成装置を用いなかったため、この対応表の計算の正当性を第三者に証明するのが容易になったためである。

第２の効果は、各計算装置の他の計算装置との通信回数が、計算する回路のゲート数に依らず定数回に留まり、効率的であることにある。

その理由は、各ゲートの入出力の対応表の対応関係がいずれの計算装置にも分からなくなる操作が必要であるが、この操作が各計算装置が順番に対応関係を入れ替える操作を行えば実現されるからである。

図面の簡単な説明

図１は非特許文献１の従来の技術を説明したフローチャートである。

図２は非特許文献１の従来の技術における、ガーブルド回路並列構築処理における、計算フェーズと通信フェーズの関係を示した図である．同じ番号が振られた計算装置が複数回記述されているが、これらは同一のもので、動作する時間が異なっているだけである．本図において、時は上から下へ流れるよう記述されている。

図３は非特許文献２の従来の技術を説明したフローチャートである。

図４は非特許文献２の従来の技術を説明したフローチャート「図(3)」における並列したランク判定処理の中で、並列して多数回行われる処理を一つだけ取り出して記述したフローチャートである。

図５は本明細書提案の技術が従来方法の問題を解決するために考案した計算処理の流れを示すブロック図である。

図６は第１の発明を実施するための最良の形態の動作の具体例を示すフローチャートである。

図７は第１の発明を実施するための最良の形態の動作の具体例における、ElGamal 暗号文準備処理の詳細を示すフローチャートの前半である。

図８は第１の発明を実施するための最良の形態の動作の具体例における、ElGamal 暗号文準備処理の詳細を示すフローチャートの後半である。

図９は第１の発明を実施するための最良の形態の動作の具体例における、逐次置換再暗号処理の詳細を示すフローチャートの前半である。右の吹き出しの中に示されたフローチャートの処理を、各計算装置が順番に行う。

図１０は第１の発明を実施するための最良の形態の動作の具体例における、結果出力処理の詳細を示すフローチャートである。

図11は第１の発明を実施するための最良の形態の構成を示すブロック図である。

図１２は第１の発明を実施するための最良の形態の構成を構成する計算装置の構成を示すブロック図である。

図１３は第１の発明を実施するための最良の形態の動作の具体例における、入力処理の詳細を示すフローチャートである。

図１４は第二の発明の装置の関係を示したブロック図、

図１５は第二の発明で、各計算装置が一周目から三周目までの各周で行う計算のフローチャート、

図１６は第二の発明におけるデータの流れ、

図１７は一周目の本計算のフローチャート、

図１８は二周目の本計算のフローチャート、

図 １９は従来の技術における各ゲートに関して計算されるデータの理解を助けるための図である。

発明を実施するための最良の形態

次に、本発明の実施例について図面を参照して説明する。

実施例１

本発明の第１の実施例について、図６ないし図１３を用いて説明する。

[準備]

[システム構成]

図１１に示すように、計算装置 308 が λ 個あり、それぞれ通信手段 307 を備えている。以下ではこの計算機を順番に、

$$\left\{u^{(\alpha)}\right\}_{\alpha=1,\ldots,\lambda}$$

と呼ぶことにする。計算装置数、各計算装置と対応する添字 α との関係等をシステムの構成情報と呼ぶ。

[回路の情報]

後の説明で、回路の情報が各計算装置

$$\left\{u^{(\alpha)}\right\}_{\alpha=1,\ldots,\lambda}$$

に入力されるが、この回路の情報を説明する。

まず、入力される回路の情報が表現する回路を f と呼ぶことにする。f は m 個の論理ゲートで構成されている回路とする。各ゲートを $G_1,\ldots,G_l,\ldots,G_m$ と呼ぶ。ここでは各ゲートは２入力１出力であるとする。この様なゲートで回路が構成されていなかった場合は、各ゲートを複数の２入力１出力のゲートからなる等価な回路に置き換える。この置き換え方法は明らかなので省略する。また回路のあるゲートから他のゲートの入力へ信号を送る配線は、0 または 1 に対応する信号を送るとする。

G「k」の出力配線を $w_{〔k〕}$ とする。fに入力される配線の本数をn個とし、これを $\{w_{〔k〕}\}_{k=m+1,\ldots,m+n}$ とする。配線は途中で分岐して二つ以上のゲートに入力していても良い。配線〔k〕は分岐しても同じ信号を送信するものとし、この分岐した配線をまとめて $w_{〔k〕}$ と呼ぶ。$w_{〔1〕},\ldots,w_{〔l〕}$ を回路fの出力とする。回路の配線は全て、ゲートの出力配線か回路への入力配線のいずれかであるので、配線全て $\{w_{〔k〕}\}_{k=1,\ldots,m+n}$ が配線の全てである。

ゲート G_k にゲート G_i とゲート G_j の出力が入力されたとき、すなわち、配線 $w_{〔i〕}$ と配線 $w_{〔j〕}$ がゲート G_k に入力され、配線 w_k が G_k の出力のための配線として繋がっているときに、G_i の出力b「i」、G_j の出力b「j」、と G_k の出力b「k」の間の関係を、$b「k」=b「i」◎_{G「k」}b「j」$ とし、各計算装置 $u^{(\alpha)}$ は、fに入力する信号の一部を持っているものとする。すなわち、配線 $\{w_{〔k〕}\}_{k=m+1,\ldots,m+n}$ のうちの一部に伝搬させる信号を知っているとする。

$u^{(\alpha)}$ がfへ入力するビットの個数を l_α 個とし、全ての計算装置の持つ入力を集めると、回路への入力全てとなるとする。すなわち、

$$\Sigma_{\alpha=1}^{\lambda} l_\alpha = \lambda$$

となる。k = m+1, ..., m+n に関して各 $w_{〔k〕}$ に入力されるビットをb「k」とし、それぞれのビットを $u^{(\alpha)}$ に l_α 個ずつ次のように割り振る。すなわち、$u^{(\alpha)}$ は集合

$$\{b「k」 \in \{0,1\} \mid k = m+\Sigma_{\beta=1}^{\alpha-1} l_\beta+1,\ldots,m+\Sigma_{\beta=1}^{\alpha} l_\beta\}$$

を決定する。ゲートの番号の割り振りを変更しても回路は本質的に変わらないため、上記のように入力を割り振っても一般性は損なわれない。

上記m個のゲート $G_1, \ldots, G_m$、それぞれのゲートの行う演算 $◎_{G[k]}$、それぞれのゲートに繋がる配線 $\{w_{〔k〕}\}_{k=m+1,\ldots,m+n}$、入力配線の計算装置に対する割り振り $\{l_\alpha\}_{\alpha=,\ldots,\lambda}$ を回路の情報300と呼ぶ。

[演算に用いる群]

本実施例では、楕円曲線上での演算を利用するのでこれを説明する。しかし、これは本発明を実施するためにはこれは必ずしも必須ではない。これに代替となるものとして、素体上の演算等、可換な乗法群であれば良い。

以降、E を位数が素数 q である楕円曲線、O を E の無限遠点、G(≠O)を E 上の点とする。q は、暗号学的に安全とされるに十分な大きさであるとする。楕円曲線 E 上の点から Z/qZ 上への写像を φ とする。φ は、その像の空間が十分に大きいものを選ぶ。φ の例として、楕円曲線 E 上の点の座標の片方の値を使う等がある。h を Z/qZ の要素、G を楕円曲線上の点としたとき、G の h 倍点を[h]G と表す。

[記法]

文字の右肩に記された文字は上付きの添字であって、冪乗を表す指数ではない。また、□は bit の排他的論理和を表すとする。

[入力処理 203,312]

処理が開始されると、図６に示されるように、まず、入力処理２０３が行なわれる。この入力処理２０３について、処理を詳細に示す図１２および図１３を参照して説明する。

ElGamal 暗号文準備処理では情報公開手段と公開情報取得手段を使って、データの公開と取得の両方を行う（309）。

[領域変数の決定]

計算は E,G 及び φ を決定する。また、ハッシュ関数を利用する等の方法で、誰もが H=[h]G なる Z/qZ の元 h が分らない様な楕円曲線上の点 H を決定する。これらの値 E, G, H, φ を領域変数 301 と呼ぶ。これらはあらかじめ全ての計算装置に格納しておく（図１３の 100）。

[回路の情報及び、回路の部分入力の入力]

回路 f の情報及びシステムの構成情報が全ての計算装置に入力される（図１３の 101）。

各計算装置 $\left\{u^{(\alpha)}\right\}_{\alpha=1,\ldots,\lambda}$ それぞれに、回路への分散された部分入力

$$\left\{b\lceil k\rfloor \in \{0,1\}\right\} k = m+\Sigma_{\beta=1}^{\alpha-1} l_\beta+1,\ldots, m+\Sigma_{\beta=1}^{\alpha} l_\beta$$

を入力する（図１３の 102）。

[ElGamal 暗号文準備処理 200,303]

[ゲート毎の秘密鍵と公開鍵設定]

次に、図６に示されるように、ElGamal 暗号文準備処理２００が行なわれる。この ElGamal 暗号文準備処理２００について、処理を詳細に示す図７および図８を参照して説明する。

各計算装置$u^{(\alpha)}$は、全ての k=1,...,m+n、全ての$b \in \{0,1\}$に関して、ゲート秘密鍵

$$X^{(\alpha)b}_{[k]} \in_R E$$

$$z^{(\alpha)} \in_R Z/qZ$$

を一様無作為に生成し（図７の 103）、全ての k=1,...,m+n、全ての$b \in \{0,1\}$に関して,

$$x^{(\alpha)b}_{[k]} = \Phi(X^{(\alpha)b}_{[k]})$$

を生成し、全ての k=1,...,m+n、全ての$b \in \{0,1\}$に関して、ゲート公開鍵

$$Y^{(\alpha)b}_{[k]} = [x^{(\alpha)b}_{[k]}]G$$

$$Z^{(\alpha)} = [z^{(\alpha)}]G$$

を生成し（図７の 104）、各計算装置u_αは各自の生成したゲート公開鍵をそれぞれ、情報公開装置を用いて公開する（図７における 105）。以降本実施例１では公開するとは、情報公開装置を用いて公開することである。

併せて計算装置$u_{(\alpha)}$は、各$Y^{(\alpha)b}_{[k]}, Z^{(\alpha)}$に関して$x^{(\alpha)b}_{[k]}, z^{(\alpha)}$の知識の証明を、別記述 A の方法に従って、ゲート公開鍵の正当性証明として生成（図７における 106）し、公開（図７の 107）する。

[入力の公開鍵設定]

各計算装置$u^{(\alpha)}$は、全ての

$$k = m+1+\Sigma_{\beta=1}{}^{\alpha-1} l_\beta, \ldots, m+\Sigma_{\beta=1}{}^{\alpha} l_\beta$$

に関して、入力された$b\ulcorner k \urcorner \in \{0,1\}$を用いて入力ゲートの秘密鍵

$$x^{\sim b\ulcorner k \urcorner}_{[k]} \in_R Z/qZ$$

を一様無作為に生成し（図７の 108）、入力ゲートの公開鍵

$$Y^{\sim b\ 「k」}{}_{[k]}=[x^{\sim b\ 「k」}{}_{[k]}]G$$
$$Y^{\sim b\ 「k」\ \square 1}{}_{[k]}=H-Y^{\sim b\ 「k」}{}_{[k]}$$

を生成し（図７の 109）、全ての$k=m+1+\Sigma_{\beta=1}{}^{\alpha-1}I_{\beta},\ldots,m+\Sigma_{\beta=1}{}^{\alpha}I_{\beta}$

全ての$b\in\{0,1\}$に関して、$Y^{\sim b}{}_{[k]}$を各計算装置の入力ゲートの公開鍵として公開する（図７の 110）。

併せて、計算装置$u_{(\alpha)}$は、各 k に関して、b「k」=0、または、b「k」=1 に対して、

$Y^{\sim b\ 「k」}{}_{[k]}=[x^{\sim b\ 「k」}{}_{[k]}]G$なる$x^{\sim b\ 「k」}{}_{[k]}$

の知識を持っていることの証明を、別記述 B の方法に従って、入力ゲートの公開鍵の正当性証明として生成（図７の 111）し、公開する（図７の 112）。

［ゲートに関する処理］

全ての計算装置$\{u_{\alpha}\}$は、公開情報取得手段を用いて、ゲート公開鍵

$$\left\{Y^{(\alpha)b}{}_{[k]},Z^{(\alpha)}\right\}_{\alpha=1,\ldots,\lambda}$$

を取得する（図８の 113）。全ての k=1,...,m と全ての$b\in\{0,1\}$に関して、各自統合したゲート公開鍵

$$Y^{b}{}_{[k]}=\Sigma_{\alpha=1}{}^{\lambda}Y^{(\alpha)b}{}_{[k]}$$
$$Z=\Sigma_{\alpha=1}{}^{\lambda}Z^{(\alpha)}$$

を生成する（図８の 114）。

全ての計算装置$\{u_{\alpha}\}$は、全ての k=1,...,m、全ての$\varepsilon\in\{0,1\}$に関して、

$$r^{(\alpha)\varepsilon}{}_{k}\in_{R}Z/qZ$$

を一様無作為に生成して、全ての k=1,...,m、全ての$b,c,\varepsilon\in\{0,1\}$に関して、楕円 ElGamal 暗号方式にて暗号化することで、ゲート秘密鍵の暗号文

$$(C^{(\alpha)bc\varepsilon}{}_{[k]},D^{(\alpha)bc\varepsilon}{}_{[k]})=([r^{(\alpha)\varepsilon}{}_{[k]}]G,X^{(\alpha)\varepsilon}{}_{[k]}+[r^{(\alpha)\varepsilon}{}_{[k]}](Y^{b}{}_{[i]}+Y^{c}{}_{[j]}+Z))$$

を生成し（図８の 115）、これらを公開する（図８の 116）。但し、ゲート G［k］

には配線 w〔i〕と w〔j〕が入力されるとする。

併せて、それぞれの k に関して、全ての $b,c \in \{0,1\}$ に関して、楕円 ElGamal 暗号文

$$(C^{(\alpha)bc0}{}_{[k]}, D^{(\alpha)bc0}{}_{[k]})$$

の復号結果が同じになること、それぞれの k に関して、全ての $b,c \in \{0,1\}$ に関して、楕円 ElGamal 暗号文

$$(C^{(\alpha)bc1}{}_{[k]}, D^{(\alpha)bc1}{}_{[k]})$$

の復号結果が同じになることの証明を、別記述 C の方法を用いて、ゲート秘密鍵の暗号文の正当性証明として生成し（図８の 117）、公開する（図８の 118）。

全ての計算装置 $\{u_\alpha\}$ は各自、全て k=1,...,m、全ての $b,c,\mu,\nu,\xi \in \{0,1\}$ に関して、秘密鍵識別データ暗号文

$$(A^{(0)bc}{}_{[k]\mu,\nu,\xi}, B^{(0)bc}{}_{[k]\mu,\nu,\xi}) = (O, [\varepsilon]G)$$

$$\{(C^{(0)\alpha bc}{}_{[k]\mu,\nu,\xi}, D^{(0)\alpha bc}{}_{[k]\mu,\nu,\xi})\}_{\alpha=1,...,\lambda} = \{(C^{(\alpha)bc\ \varepsilon}{}_{[k]}, D^{(\alpha)bc\ \varepsilon}{}_{[k]})\}_{\alpha=1,...,\lambda}$$

を生成する（図８の 119）。但し、

$$\varepsilon = ((b \square \mu) \circledcirc_G {}^{\lceil k \rfloor}(c \square \nu)) \square \xi .$$

〔入力配線に関する処理〕

全ての計算装置 $\{u_\alpha\}$ は、全ての k=m+1,...,m+n、全ての $\varepsilon \in \{0,1\}$ に関して

$$r^{\sim(\alpha)\varepsilon}{}_k \in_R Z/qZ$$

を一様無作為に生成し、全ての k=m+1,...,m+n、全ての $b,\varepsilon \in \{0,1\}$ に関して楕円 ElGamal 暗号方式を用いて、入力の暗号文

$$(C^{(\alpha)bc\varepsilon}{}_{[k]}, D^{(\alpha)bc\varepsilon}{}_{[k]}) = ([r^{\sim(\alpha)\varepsilon}{}_{[k]}]G, X^{(\alpha)\varepsilon}{}_{[k]} + [r^{\sim(\alpha)\varepsilon}{}_{[k]}](Y^{\sim b}{}_{[k]} + Z))$$

を生成し（図８の 120）、これらを公開する（図８の 121）。併せて、それぞれの k に関して、全ての $b \in \{0,1\}$ に関して、楕円 ElGamal 暗号文

$$(C^{(\alpha)bc0}{}_{[k]}, D^{(\alpha)b0}{}_{[k]})$$

の復号結果が同じになること、それぞれの k に関して、全ての $b \in \{0,1\}$ に関して、楕円 ElGamal 暗号文

$$(C^{(\alpha)b1}{}_{[k]}, D^{(\alpha)b1}{}_{[k]})$$

の復号結果が同じになることの証明を、別記述 D の方法で、入力の暗号文の正当性証明として生成し（図８の 122)、公開する（図８の 123)。

全ての計算装置{u_α}は各自、全ての k=m+1,...,m+n、全ての$b,\xi\in\{0,1\}$に関して、入力の暗号文識別データの暗号文

$$(A^{(0)b}{}_{[k]\xi}, B^{(0)b}{}_{[k]\xi}) = (O,[\varepsilon]G)\ \{(C^{(0)\alpha b}{}_{[k]\xi}, D^{(0)\alpha b}{}_{[k]\xi})\}_{\alpha=1,\ldots,\lambda} = \{(C^{(\alpha)b\varepsilon}{}_{[k]}, D^{(\alpha)b\varepsilon}{}_{[k]})\}_{\alpha=1,\ldots,\lambda}$$

を生成する（図８の 124)。但し$\varepsilon = b\square\xi$.

[出力配線に関する処理]

全ての計算装置{u_α}は各自、全ての配線 k=1,...,l、全ての$b,\varepsilon\in\{0,1\}$に関して、出力の暗号文

$$(A^{\dagger(0)b}{}_{[k]\xi}, B^{\dagger(0)b}{}_{[k]\xi}),\ \&=\&\ (O,[\varepsilon]G)$$

を生成する（図８の 125)。但し$\varepsilon = b\square\xi$.

[逐次置換再暗号処理 201 --- ゲート暗号文の置換と再暗号]

次に、図６に示されるように、逐次置換再暗号処理２０１が行なわれる。この逐次置換再暗号処理２０１について、処理を詳細に示す図９および図１２を参照して説明する。

$\alpha=1,\ldots,\lambda$に関して順番に、計算装置u_αは以下の処理（図１２の 304）を行う（図９の 126)。この処理で各計算装置は、最初に公開情報取得手段を用いて必要なデータを取得し（図１２の 310)、次に生成したデータを情報公開手段を用いて公開する（図１２の 311)。λ個の計算装置には順番が定められており、それぞれの計算装置がデータを取得するには、この計算機よりも順番が前の計算機全てがデータの公開を終了しておかねばならない。

[暗号文取得処理]

u_αは、k=1,...,m、全ての$\beta=1,\ldots,\lambda$、全ての$b,c,\mu,\nu,\xi\in\{0,1\}$に関する

$$A^{(\alpha-1)bc}{}_{[k]\ \mu,\nu,\xi}, B^{(\alpha-1)bc}{}_{[k]\ \mu,\nu,\xi}, C^{(\alpha-1)\beta bc}{}_{[k]\ \mu,\nu,\xi}, D^{(\alpha-1)\beta bc}{}_{[k]\ \mu,\nu,\xi},$$

全ての k=m+1,...,m+n、全ての$\beta=1,\ldots,\lambda$、全ての$b,\xi\in\{0,1\}$に関する

$A^{(\alpha-1)b_{[k]}}\xi, B^{(\alpha-1)b_{[k]}}\xi, C^{(\alpha-1)\beta b_{[k]}}\xi, D^{(\alpha-1)\beta b_{[k]}}\xi,$

全ての k=1,...,l、全ての $b,\xi \in \{0,1\}$ に関する

$A^{\dagger(\alpha-1)b_{[k]}}\xi, B^{\dagger(\alpha-1)b_{[k]}}\xi$

を取得する（図９の 151）。

［配線の信号値と置換生成］

u_α は、各配線の信号値の置換 $\{\pi(k) \in_R \{0,1\}\}_{k=1,\ldots,m+n}$ を一様無作為に生成する（図９の 127）。

［再暗号化の乱数生成］

u_α は、ゲートの秘密鍵の再暗号化に使う乱数

$$\{s^{(\alpha)bc}_{[k]}\mu,\nu,\xi\}_{k=1,\ldots,m;b,c,\mu,\nu,\xi \in R\{0,1\}}$$

$$\{t^{(\alpha)\beta bc}_{[k]}\mu,\nu,\xi\}_{k=1,\ldots,m;\beta=1,\ldots,\beta;b,c,\mu,\nu,\xi \in R\{0,1\}}$$

$$\{s^{(\alpha)b}_{[k]}\xi\}_{k=m+1,\ldots,m+n;b,\xi \in R\{0,1\}}$$

$$\{t^{(\alpha)\beta b}_{[k]}\xi\}_{k=m+1,\ldots,m+n;\beta=1,\ldots,\lambda;b,\xi \in R\{0,1\}}$$

$$\{s^{\dagger b}_{[k]}\xi\}_{k=1,\ldots,l;b,\xi \in R\{0,1\}}$$

を一様無作為に生成する（図９の 128）。

［ゲートの秘密鍵の暗号文の置換と再暗号化］

全ての k=1,...,m、全ての β=1,...,λ、全ての $b,c,\mu,v,\xi \in \{0,1\}$ に関して、

$$A^{(\alpha)bc}{}_{[k]\mu,\nu,\xi} = A^{(\alpha-1)bc}{}_{[k]\mu\,\square\,\pi(i),\nu\,\square\,\pi(j),\xi\,\square\,\pi(k)} + [s^{(\alpha)bc}{}_{[k]\mu,\nu,\xi}]G$$

$$B^{(\alpha)bc}{}_{[k]\mu,\nu,\xi} = B^{(\alpha-1)bc}{}_{[k]\mu\,\square\,\pi(i),\nu\,\square\,\pi(j),\xi\,\square\,\pi(k)} + [s^{(\alpha)bc}{}_{[k]\mu,\nu,\xi}](Y^{b}{}_{[i]} + Y^{c}{}_{[j]} + Z)$$

$$C^{(\alpha)\beta\,bc}{}_{[k]\mu,\nu,\xi} = C^{(\alpha-1)\beta\,bc}{}_{[k]\mu\,\square\,\pi(i),\nu\,\square\,\pi(j),\xi\,\square\,\pi(k)} + [t^{(\alpha)\beta\,bc}{}_{[k]\mu,\nu,\xi}]G$$

$$D^{(\alpha)\beta\,bc}{}_{[k]\mu,\nu,\xi} = D^{(\alpha-1)\beta\,bc}{}_{[k]\mu\,\square\,\pi(i),\nu\,\square\,\pi(j),\xi\,\square\,\pi(k)} + [t^{(\alpha)\beta\,bc}{}_{[k]\mu,\nu,\xi}](Y^{b}{}_{[i]} + Y^{c}{}_{[j]} + Z)$$

と、ゲート秘密鍵を置換し再暗号化したデータを生成し（図９の 129)、

［入力の暗号文の置換と再暗号化］

全ての k=m+1,...,m+n、全ての β=1,...,λ、全ての b,ξ ∈ {0,1} に関して、

$$A^{(\alpha)b}{}_{[k]\xi} = A^{(\alpha-1)b}{}_{[k]\xi\,\square\,\pi(k)} + [s^{(\alpha)b}{}_{[k]\xi}]G$$

$$B^{(\alpha)b}{}_{[k]\xi} = B^{(\alpha-1)\,b}{}_{[k]\xi\,\square\,\pi(k)} + [s^{(\alpha)b}{}_{[k]\xi}](Y^{\sim b}{}_{[k]} + Z)$$

$$C^{(\alpha)\beta\,b}{}_{[k]\xi} = C^{(\alpha-1)\beta\,b,sub>[k]\xi\,\square\,\pi(k)} + [t^{(\alpha)b}{}_{[k]\xi}]G$$

$$D^{(\alpha)\beta\,b}{}_{[k]\xi} = D^{(\alpha-1)\beta\,b}{}_{[k]\xi\,\square\,\pi(k)} + [t^{(\alpha)b}{}_{[k]\xi}](Y^{\sim b}{}_{[k]} + Z)$$

と、入力の暗号文を置換し再暗号化したデータを生成し（図９の 130)、

［出力の暗号文の置換と再暗号化］

全ての k=1,...,l、全ての b,ξ ∈ {0,1} に関して,

$$A^{\dagger(\alpha)b}{}_{[k]\xi} = A^{\dagger(\alpha-1)b}{}_{[k]\xi\,\square\,\pi(k)} + [s^{\dagger b}{}_{[k]\xi}]G$$

$$B^{\dagger(\alpha)b}{}_{[k]\xi} = B^{\dagger(\alpha-1)b}{}_{[k]\xi\,\square\,\pi(k)} + [s^{\dagger b}{}_{[k]\xi}](Y^{b}{}_{[k]} + Z)$$

と、出力の暗号文を置換し再暗号化したデータを生成し（図９の 131)、

［置換と再暗号化の正当性証明］全ての k=1,...,m、全ての β=1,...,λ、全ての b,c,μ,ν,ξ ∈ {0,1} に関する

$\{A^{(\alpha)bc}{}_{[k]\ \mu,\nu,\xi}, B^{(\alpha)bc}{}_{[k]\ \mu,\nu,\xi}, C^{(\alpha)\beta bc}{}_{[k]\ \mu,\nu,\xi}, D^{(\alpha)\beta bc}{}_{[k]\ \mu,\nu,\xi}\}$

及び、全ての $k=m+1,...,m+n$、全ての $\beta=1,...,\lambda$、全ての $b,\xi\in\{0,1\}$ に関する

$\{A^{(\alpha)b}{}_{[k]\ \xi}, B^{(\alpha)b}{}_{[k]\ \xi}, C^{(\alpha)\beta b}{}_{[k]\ \xi}, D^{(\alpha)\beta b}{}_{[k]\ \xi}\}$

及び全ての $k=1,...,l$、全ての $b,\xi\in\{0,1\}$ に関する $A^{\dagger(\alpha)b}{}_{[k]\ \xi}, B^{\dagger(\alpha)b}{}_{[k]\ \xi}$ を

$u_{\alpha+1}$ に送信する。

併せて上記処理を正当に行ったことの証明を、別記述 E の方法に従って、ゲートの秘密鍵の暗号文と入力の暗号文と出力の暗号文との置換と再暗号化の正当性証明として生成し公開する（図９の 132）。

[結果出力処理 202,305]

次に、図６に示されるように、結果出力処理２０２が行なわれる。この結果出力処理２０２について、処理を詳細に示す図１０ないし図１２を参照して説明する。

結果出力処理２０２では情報公開手段と公開情報取得手段を使って、データの公開と取得の両方を行う（図１２の 312）。最後に、各自回路の出力（図１２の 306）を出力する（図１２の 313）。

[ゲート暗号文の部分復号]

全ての計算装置 $\{u_\alpha\}_{\alpha=1,...,\lambda}$ は、全ての $k=1,...,m, b,c\in\{0,1\}, \beta=1,...,\lambda$ に関して、

$$A^{\ddagger(\lambda)\alpha bc}{}_{[k]000}=[z^{(\alpha)}]A^{(\lambda)bc}{}_{[k]000}$$
$$C^{\ddagger(\lambda)\alpha\beta bc}{}_{[k]000}=[z^{(\alpha)}]C^{(\lambda)\beta bc}{}_{[k]000}$$

と、ゲート秘密鍵を部分復号し、結果を公開し（図１０の 134）、全ての計算装置 $\{u_\alpha\}_{\alpha=1,...,\lambda}$ は、全ての $k=m+1,...,m+n, b\in\{0,1\}, \beta=1,...,\lambda$ に関して

$$A^{\ddagger(\lambda)\alpha b}{}_{[k]0}=[z^{(\alpha)}]A^{(\lambda)b}{}_{[k]0}$$
$$C^{\ddagger(\lambda)\alpha\beta b}{}_{[k]0}=[z^{(\alpha)}]C^{(\lambda)\beta b}{}_{[k]0}$$

と、入力の暗号文を部分復号し、結果を公開し（図１０の 135）、全ての計算装置 $\{u_\alpha\}_{\alpha=1,...,\lambda}$ は、$k=1,...,l, b\in\{0,1\}$ に関して

$$A^{\dagger\ddagger(\lambda)\alpha b}{}_{[k]0}=[z^{(\alpha)}]A^{\dagger(\lambda)b}{}_{[k]0}$$

と、出力の暗号文を部分復号し、結果を公開する（図１０の 136）。

併せて上記処理を正当に行ったことの証明を別記述Ｆの方法に従って、ゲート秘密鍵と入力の暗号文と出力の暗号文との部分復号の正当性証明として生成し公開する（図１０の 137）。

［ゲート暗号文の生成］

全ての計算装置は、さらに全ての k=1,...,m、全ての α=1,...,λ、全ての b,c,∈{0,1}に関して、

$$A^{bc}[k] = A^{(\lambda)bc}[k]000$$
$$B^{bc}[k] = B^{(\lambda)bc}[k]000 - \Sigma_{\alpha=1}{}^{\lambda} A^{\sharp(\lambda)\alpha bc}[k]000$$
$$C^{\alpha bc}[k] = C^{(\lambda)\alpha bc}[k]000$$
$$D^{\alpha bc}[k] = D^{(\lambda)\alpha bc}[k]000 - \Sigma_{\alpha=1}{}^{\lambda} C^{\sharp(\lambda)\alpha\beta bc}[k]000$$

を、全ての k=m+1,...,m+n、全ての α=1,...,λ、全ての b∈{0,1}に関して、

$$A^{b}[k] = A^{(\lambda)b}[k]0$$
$$B^{b}[k] = B^{(\lambda)b}[k]0 - \Sigma_{\alpha=1}{}^{\lambda} A^{\sharp(\lambda)\alpha b}[k]0$$
$$C^{\alpha b}[k] = C^{(\lambda)\alpha b}[k]0$$
$$D^{\alpha b}[k] = D^{(\lambda)\alpha b}[k]0 - \Sigma_{\alpha=1}{}^{\lambda} C^{\sharp(\lambda)\alpha\beta b}[k]0$$

を、全ての k=1,...,l、全ての b∈{0,1}に関して、

$$A^{\dagger b}[k] = A^{\dagger(\lambda)b}[k]0$$
$$B^{\dagger b}[k] = B^{\dagger(\lambda)b}[k]0 - A^{\dagger\sharp(\lambda)\alpha b}[k]0$$

をゲート暗号文として生成する（図１０の 138）。

［入力の復号］

各計算装置 $u^{(\alpha)}$は、全ての $k = m+1+\Sigma_{\gamma=1}{}^{\alpha-1} l_\gamma,...,m+\Sigma_{\gamma=1}{}^{\alpha} l_\gamma$、全ての β=1,...,λ

に関して、b「k」を開示することなく

$$G^{b}{}_{[k]}=B^{b\lceil k\rfloor}{}_{[k]}-[x^{\sim b\lceil k\rfloor}{}_{[k]}]A^{b\lceil k\rfloor}{}_{[k]}$$

$$X^{b}(\beta)_{[k]}=D^{\beta\, b\lceil k\rfloor}{}_{[k]}-[x^{\sim b\lceil k\rfloor}{}_{[k]}]C^{\beta\, b\lceil k\rfloor}{}_{[k]}$$

$$x^{b}(\beta)_{[k]}=\phi(X^{b}(\beta)_{[k]})$$

を生成し、公開する（図１０の 139)。この公開したデータは入力の暗号文を復号したデータと呼ぶ。

全ての計算装置u_αは、全ての k=m+1,...,m+n、全ての β=1,...,λ に関して、

$$Y^{(\beta)\varepsilon\ \lceil k\rfloor}{}_{[k]}=[x^{b(\beta)}{}_{[k]}]G$$

を確認することで、入力の暗号文の復号の正当性を確認する（図１０の 140)。但し、もし$G^{b}{}_{[k]}=0$なら$\varepsilon_k=0$, $G^{b}{}_{[k]}=G$なら$\varepsilon_k=1$とする。

[回路の評価]

全ての計算装置u_αはそれぞれ、全てのゲート $G_{kk=1,...,m}$ に関して適切な順番に、それらの入力から出力を以下のように求めていく（図１０の 141)。これが回路の評価の処理である。但しゲート G_k にはゲート G_i とゲート G_j の出力が入力されるとする。

全ての β=1,...,λ に関して,

$$G^{b}{}_{[k]}=B^{b\lceil i\rfloor b\lceil j\rfloor}{}_{[k]}-[\Sigma_{\gamma=1}\lambda(x(\gamma)b\lceil i\rfloor_{[k]}+x(\gamma)b\lceil j\rfloor_{[k]})]\,A^{b\lceil i\rfloor b\lceil j\rfloor}{}_{[k]}$$

$$X^{b}(\beta)_{[k]}=D^{\beta\ b\lceil i\rfloor\, b\lceil j\rfloor}{}_{[k]}-[\Sigma_{\gamma=1}\lambda(x(\gamma)b\lceil i\rfloor_{[k]}+x(\gamma)b\lceil j\rfloor_{[k]})]\,C^{\beta\ b\lceil i\rfloor\, b\lceil j\rfloor}{}_{[k]}$$

$$x^{b}(\beta)_{[k]}=\phi(X^{b}(\beta)_{[k]})$$

を求め（図１０の 142)、β=1,...,λ に関して, $Y^{(\beta)\varepsilon\ \lceil k\rfloor}{}_{[k]}=[x^{b(\beta)}{}_{[k]}]G$ を確認する（図１０の 143)。但し、もし$G^{b}{}_{[k]}=0$なら$\varepsilon_k=0$, $G^{b}{}_{[k]}=G$なら$\varepsilon_k=1$とする。上記処理を行った k に関して、b「k」= ε_k とする。

[出力の評価]

ここまでの処理で公開した証明を検証者は検証する（図１０の 144)。検証者が全ての証明文を受理したならば、すなわち不正が発見されなかったならば、以下の

出力の復号と公開の処理を行う。

全ての計算装置u_αはそれぞれ、全ての k=1,...,l に関して,

$$G^{\dagger}_{[k]}=B^{\dagger b\lceil k\rfloor}_{[k]}-[\Sigma_{\gamma=1}{}^{\lambda}(x^{(\gamma)b\lceil k\rfloor}_{[k]}]\,A^{\dagger b\lceil k\rfloor}_{[k]}$$

を求める（図１０の 145)。

全ての$\{u_\alpha\}_{\alpha=1,\ldots,\lambda}$はそれぞれ、全ての k=1,...,l に関して,

$$A^{\dagger\sharp}_{[k]}=[z^{(\alpha)}]A^{\dagger b\ \lceil k\rfloor}_{[k]}$$

を生成して（図１０の 146）公開する（図１０の 147)。

併せてこの計算の正当性の証明を、別記述 G の方法に従って、出力の復号の正当性の証明生成と（図１０の 148）して公開する（図１０の 149)。

それぞれのu_αは、各自

$$G^{\text{♪}}_{[k]}=G^{\dagger}_{[k]}-\Sigma_{\gamma=1}{}^{\lambda}A^{\dagger\sharp}_{[k]}$$

から回路の出力（図 11 の 306）を求める（図１０の 150)。

k=1,...,l に関して、$G^{\text{♪}}_{[k]}=0$ならば b「k」=0 であり、$G^{\text{♪}}_{[k]}=G$ならば b「k」=1 である。

[別記述処理]

[別記述 A]

証明者(計算者) u_αは、全ての k=1,...,m+n、全ての$b\in\{0,1\}$に関して,

$$x'^{(\alpha)b}_{[k]}\in_R Z\setminus qZ$$

$$z'^{(\alpha)}_{[k]}\in_R Z\setminus qZ$$

を一様無作為に生成し,

$$Y'^{(\alpha)b}_{[k]}\in[x'^{(\alpha)b}_{[k]}]G$$

$$Z'^{(\alpha)}=[z'^{(\alpha)}]G$$

を生成する。さらに,

$$\theta=\mathrm{Hash}(E,G,[Y^{(\alpha)b}_{[k]}]_{k=1,\ldots,m+n;b=0,1},Z^{(\alpha)},[Y'^{(\alpha)b}_{[k]}]_{k=1,\ldots,m+n;b=0,1},Z'^{(\alpha)})\bmod q$$

を生成し、全ての k=1,...,m+n、全ての$b\in\{0,1\}$に関して、

$x''(\alpha)b_{[k]} = \theta\ x(\alpha)b_{[k]} + x'(\alpha)b_{[k]} \bmod q$

$z''(\alpha) = \theta\ z(\alpha) + z'(\alpha) \bmod q$

を生成する。証明者は、全ての k=1,...,m+n、全てのb∈{0,1}に関する

$Y''(\alpha)b_{[k]}, Z'(\alpha), z(\alpha)b_{[k]}, z''(\alpha)$

を証明とする。上記証明の検証方法は以下の通り。検証者は、

$\theta = \mathrm{Hash}(E,G,\{Y(\alpha)b_{[k]}\}_{k=1,...,m+n;b=0,1}, Z(\alpha), \{Y'(\alpha)b_{[k]}\}_{k=1,...,m+n;b=0,1}, Z'(\alpha)) \bmod q$

を計算して、

$[x''(\alpha)b_{[k]}]G = [\theta]\,Y(\alpha)b_{[k]} + Y'(\alpha)b_{[k]}$

$[z''(\alpha)]G = \theta\ Z(\alpha) + Z'(\alpha)$

を確認する。

[別記述 B]

各証明者(計算者) $u^{(\alpha)}$ は、全ての $k = m+1+\Sigma_{\beta=1}^{\alpha-1} l_\beta, \ldots, m+\Sigma_{\beta=1}^{\alpha} l_\beta$ に関して、選択したb「k」$\in\{0,1\}$に対して,

$\tilde{x}'b\ 「k」_{[k]} \in_R Z/qZ$

を一様無作為に生成し、

$\tilde{Y}'b\ 「k」_{[k]} = [\tilde{x}'b\ 「k」_{[k]}]G$

を生成する。さらに、

$\theta b「k」□1_{[k]} \in_R Z/qZ$

$\tilde{x}''b「k」□1_{[k]} \in_R Z/qZ$

を無作為に生成し,

$\tilde{Y}''b「k」□1_{[k]} = [\tilde{x}''b「k」□1_{[k]}]G - [\theta b「k」□1_{[k]}]\,\tilde{Y}b「k」□1_{[k]}$

を生成する。

u_αは、全ての$k = m+1+\Sigma_{\beta=1}^{\alpha-1} I_\beta, \ldots, m+\Sigma_{\beta=1}^{\alpha} I_\beta$に関して、

$$\theta_{[k]} = \mathrm{Hash}(E, G, \{Y^{\sim b}_{[k]}, Y^{\sim b}_{[k]}\}_{b=0,1}) \bmod q$$

$$\theta^{b\lceil k \rfloor}_{[k]} = \theta_{[k]} - \theta^{b\lceil k \rfloor \square 1}_{[k]} \bmod q$$

を生成する。さらに、

$$x^{\sim\sim b\lceil k \rfloor}_{[k]} = \theta^{b\lceil k \rfloor}_{[k]} x^{\sim b\lceil k \rfloor}_{[k]} + x^{\sim\sim b\lceil k \rfloor}_{[k]} \bmod q$$

を生成する。

証明者u_αは、全ての$k = m+1+\Sigma_{\beta=1}^{\alpha-1} I_\beta, \ldots, m+\Sigma_{\beta=1}^{\alpha} I_\beta, b = 0,1$に関する

$$Y^{\sim' b}_{[k]}, \theta^{0}_{[k]}, x^{\sim'' b}_{[k]}$$

を証明とする。

上記証明の検証方法は以下の通り。

検証者は、全ての

$$k = m+1+\Sigma_{\beta=1}^{\alpha-1} I_\beta, \ldots, m+\Sigma_{\beta=1}^{\alpha} I_\beta, b = 0,1$$

に関して、

$$\theta_{[k]} = \mathrm{Hash}(E, G, \{Y^{\sim b}_{[k]}, Y^{\sim' b}_{[k]}\}_{b=0,1}) \bmod q$$

$$\theta^{1}_{[k]} = \theta_{[k]} - \theta^{0}_{[k]} \bmod q$$

を生成し、全ての

$$k=m+1+\Sigma_{\beta=1}^{\alpha-1} I_\beta, \ldots, m+\Sigma_{\beta=1}^{\alpha} I_\beta, b=0,1$$

に関して、

$$[x''^{b}_{[k]}]G = [\theta^{b}_{[k]}]\, Y^{b}_{[k]} + Y''^{b}_{[k]}$$

$$Y^{0}_{[k]} + Y^{1}_{[k]} = H$$

が成り立つことを確認する。

[別記述 C]

証明者(計算者) u_α は、全ての k=1,...,m、全ての ε=0,1 に関して、

$$r'(\alpha)\varepsilon 0_{[k]} \in Z/qZ$$

を一様無作為に生成して、

$$F(\alpha)\varepsilon 0_{[k]} = [r'(\alpha)\varepsilon 0_{[k]}]G$$

$$F(\alpha)\varepsilon 1_{[k]} = [r'(\alpha)\varepsilon 1_{[k]}]\,(Y^{1}_{[i]} - Y^{0}_{[i]})$$

$$F(\alpha)\varepsilon 2_{[k]} = [r'(\alpha)\varepsilon 2_{[k]}]\,(Y^{1}_{[j]} - Y^{0}_{[j]})$$

を生成する。

さらに、

$$\theta(\alpha)_{[k]'} = \mathrm{Hash}\,(E,G,\{C(\alpha)bc\ \varepsilon_{[k]'}\, D(\alpha)bc\ \varepsilon_{[k]}\}_{k=1,...,m;b,c,\varepsilon=0,1'}\{F(\alpha)\varepsilon 0_{[k]'}\, F(\alpha)\varepsilon 1_{[k]'}\, F(\alpha)\varepsilon 2_{[k]'}\}_{k=1,...,m;\varepsilon=0,1})$$

を生成する。

次に、

$$r''(\alpha)\varepsilon_{[k]} = \theta(\alpha)_{[k]}\, r(\alpha)\varepsilon_{[k]} + r'(\alpha)\varepsilon_{[k]} \bmod q$$

を生成する。証明者は、k=1,...,m 及び ε=0,1 に関する

$$F(\alpha)\varepsilon 0_{[k]'}\, F(\alpha)\varepsilon 1_{[k]'}\, F(\alpha)\varepsilon 2_{[k]'}\, r''(\alpha)\varepsilon_{[k]}$$

を証明とする。

上記証明の検証方法は以下の通り。

検証者は、最初にそれぞれの ε=0,1、及び k=1,...,m に関して、全ての b,c=0,1 に対する

$C^{(\alpha)bc\varepsilon}{}_{[k]}$が全て同じ値であることを確認する。

次に、

$$\theta(\alpha)_{[k]}, = \mathrm{Hash}\,(E,G,\,[\,C^{(\alpha)bc}\,\varepsilon_{[k]},\,D^{(\alpha)bc}\,\varepsilon_{[k]}\,]_{k=1,\ldots,m;b,c,\,\varepsilon=0,1},\,[\,F^{(\alpha)}\varepsilon 0_{[k]},\,F^{(\alpha)}\varepsilon 1_{[k]},\,F^{(\alpha)}\varepsilon 2_{[k]},\,]_{k=1,\ldots,m;\,\varepsilon=0,1}\,)$$

を生成する。次に、すべての k=1,...,m 及び ε=0,1 に関して

$$[r''^{(\alpha)}\varepsilon_{[k]}]G = [\theta(\alpha)_{[k]}]\,C^{(\alpha)00}\varepsilon_{[k]} + F^{(\alpha)}\varepsilon 0_{[k]}$$

$$[r''^{(\alpha)}\,\varepsilon_{[k]}]\,(Y^1{}_{[j]} - Y^0{}_{[j]}) = [\theta(\alpha)_{[k]}]\,(D^{(\alpha)01}\,\varepsilon_{[k]} - D^{(\alpha)00}\varepsilon_{[k]}) + F^{(\alpha)}\varepsilon 2_{[k]}$$

$$[r''^{(\alpha)}\,\varepsilon_{[k]}]\,(Y^1{}_{[i]} - Y^0{}_{[i]}) = [\theta(\alpha)_{[k]}]\,(D^{(\alpha)10}\,\varepsilon_{[k]} - D^{(\alpha)00}\varepsilon_{[k]}) + F^{(\alpha)}\varepsilon 1_{[k]}$$

$$(D^{(\alpha)11}\,\varepsilon_{[k]} - D^{(\alpha)10}\,\varepsilon_{[k]}) = (D^{(\alpha)01}\,\varepsilon_{[k]} - D^{(\alpha)00}\varepsilon_{[k]})$$

が成り立つことを確認する。

[別記述 D]

証明者(計算者)uα は、全ての k=m+1,...,m+n、全ての b,ε=0,1 に関して、

$$r'^{(\alpha)}b_{[k]} \in Z/qZ$$

を一様無作為に生成して,

$$F^{(\alpha)}\varepsilon 0_{[k]} = [\tilde{r}'^{(\alpha)}\,\varepsilon_{[k]}]G$$

$$F^{(\alpha)}\varepsilon 1_{[k]} = [\tilde{r}'^{(\alpha)}\,\varepsilon_{[k]}]\,(\tilde{Y}^1{}_{[k]} - \tilde{Y}^0{}_{[k]})$$

を生成する。さらに、全ての k=m+1,...,m+n に関して

$$\theta(\alpha)_{[k]}, = \mathrm{Hash}\,(E,G,\,[\,C^{(\alpha)b}\,\varepsilon_{[k]},\,D^{(\alpha)b}\,\varepsilon_{[k]},\,F^{(\alpha)b}\,\varepsilon_{[k]}\,]_{k=m+1,\ldots,m+n;b,\,\varepsilon=0,1}\,)$$

を生成する。

次に、全ての k=m+1,...,m+n、全ての b,ε=0,1 に関して,

$$r''(\alpha)\varepsilon_{[k]} = \theta(\alpha)_{[k]}\, r(\alpha)\varepsilon_{[k]} + r''(\alpha)\varepsilon_{[k]} \bmod q$$

を生成する。証明者は、k=m+1,...,m+n 及び ε=0,1 に関する

$$F(\alpha)\varepsilon 0_{[k]},\ F(\alpha)\varepsilon 1_{[k]},\ r''(\alpha)\varepsilon_{[k]}$$

を証明とする。

上記証明の検証方法は以下の通り。検証者は、最初にそれぞれの ε=0,1、及び k=1,...,m に関して、全ての b=0,1 に対する

$$C(\alpha)b\varepsilon_{[k]}$$

が全て同じ値であることを確認する。

次に、

$$\theta(\alpha)_{[k]}, = \mathrm{Hash}\,(E,G,\{C(\alpha)b\varepsilon_{[k]}, D(\alpha)b\varepsilon_{[k]}, F(\alpha)b\varepsilon_{[k]}\}_{k=m+1,...,m+n;b,\varepsilon=0,1})$$

を生成する。

次に、すべての k=m+1,...,m+n 及び ε=0,1 に関して

$$[r''(\alpha)\varepsilon_{[k]}]G = [\theta(\alpha)_{[k]}]\, C(\alpha)0\varepsilon_{[k]} + F(\alpha)\varepsilon 0_{[k]}$$

$$[r''(\alpha)\varepsilon_{[k]}]\,(Y^{1}_{[j]} - Y^{0}_{[j]}) = [\theta(\alpha)_{[k]}]\,(D(\alpha)1\varepsilon_{[k]} - D(\alpha)0\varepsilon_{[k]}) + F(\alpha)\varepsilon 1_{[k]}$$

が成り立つことを確認する。

[別記述 E]

α=1,...,λ に関して順番に、計算者 u_α は以下の処理を行う。

u_α は、

$$\Sigma_{h=0,1/3,2/3}\ \sigma(\alpha-h)bc_{[k]}\mu,\nu,\xi = s(\alpha)bc_{[k]}\mu,\nu,\xi \bmod q$$

$$\Sigma_{h=0,1/3,2/3}\ \tau(\alpha-h)\beta\, bc_{[k]}\mu,\nu,\xi = t(\alpha)\beta\, bc_{[k]}\mu,\nu,\xi \bmod q$$

なる

$[\sigma^{(\alpha-h)bc}{}_{[k]\mu,\nu,\xi}, \tau^{(\alpha-h)\beta bc}{}_{[k]\mu,\nu,\xi}]_{k=1,...,m;\beta=1,...,\lambda;h=2/3,1/3,0;b,c,\mu,\nu,\xi\in\{0,1\}}$

を Z/qZ から一様無作為に選び,全ての k=1,...,m、全ての b,c,μ,v,ξ∈{0,1}に関して,

$A^{(\alpha-2/3)bc}{}_{[k]\mu,\nu,\xi} = A^{(\alpha-1)bc}{}_{[k]\mu\square\pi(i),\nu,\xi} + [\sigma^{(\alpha-2/3)bc}{}_{[k]\mu,\nu,\xi}]G$

$B^{(\alpha-2/3)bc}{}_{[k]\mu,\nu,\xi} = B^{(\alpha-1)bc}{}_{[k]\mu\square\pi(i),\nu,\xi} + [\sigma^{(\alpha-2/3)bc}{}_{[k]\mu,\nu,\xi}](Y^b{}_{[i]}+Y^c{}_{[j]}+Z)$

$C^{(\alpha-2/3)\beta\ bc}{}_{[k]\mu,\nu,\xi} = C^{(\alpha-1)\beta bc}{}_{[k]\mu\square\pi(i),\nu\ \xi} + [\tau^{(\alpha-2/3)\beta\ bc}{}_{[k]\mu,\nu,\xi}]G$

$D^{(\alpha-2/3)\beta\ bc}{}_{[k]\mu,\nu,\xi} = D^{(\alpha-1)\beta bc}{}_{[k]\mu\square\pi(i),\nu,\xi} + [\tau^{(\alpha-2/3)\beta\ bc}{}_{[k]\mu,\nu,\xi}](Y^b{}_{[i]}+Y^c{}_{[j]}+Z)$

$A^{(\alpha-1/3)bc}{}_{[k]\mu,\nu,\xi} = A^{(\alpha-2/3)bc}{}_{[k]\mu,\nu\square\pi(j),\xi} + [\sigma^{(\alpha-1/3)bc}{}_{[k]\mu,\nu,\xi}]G$

$B^{(\alpha-1/3)bc}{}_{[k]\mu,\nu,\xi} = B^{(\alpha-2/3)bc}{}_{[k]\mu,\nu\square\pi(j),\xi} + [\sigma^{(\alpha-1/3)bc}{}_{[k]\mu,\nu,\xi}](Y^b{}_{[i]}+Y^c{}_{[j]}+Z)$

$C^{(\alpha-1/3)\beta\ bc}{}_{[k]\mu,\nu,\xi} = C^{(\alpha-2/3)\beta\ bc}{}_{[k]\mu,\nu\square\pi(j),\xi} + [\tau^{(\alpha-1/3)\beta\ bc}{}_{[k]\mu,\nu,\xi}]G$

$D^{(\alpha-1/3)\beta\ bc}{}_{[k]\mu,\nu,\xi} = D^{(\alpha-2/3)\beta\ bc}{}_{[k]\mu,\nu\square\pi(j),\xi} + [\tau^{(\alpha-1/3)\beta\ bc}{}_{[k]\mu,\nu,\xi}](Y^b{}_{[i]}+Y^c{}_{[j]}+Z)$

$A^{(\alpha)bc}{}_{[k]\mu,\nu,\xi} = A^{(\alpha-1/3)bc}{}_{[k]\mu,\nu\square\pi(j),\xi} + [\sigma^{(\alpha)bc}{}_{[k]\mu,\nu,\xi}]G$

$B^{(\alpha)bc}{}_{[k]\mu,\nu,\xi} = B^{(\alpha-1/3)bc}{}_{[k]\mu,\nu\square\pi(j),\xi} + [\sigma^{(\alpha)bc}{}_{[k]\mu,\nu,\xi}](Y^b{}_{[i]}+Y^c{}_{[j]}+Z)$

$C^{(\alpha)\beta bc}{}_{[k]\mu,\nu,\xi} = C^{(\alpha-1/3)\beta\ bc}{}_{[k]\mu,\nu\square\pi(j),\xi} + [\tau^{(\alpha)\beta bc}{}_{[k]\mu,\nu,\xi}]G$

$D^{(\alpha)\beta bc}{}_{[k]\mu,\nu,\xi} = D^{(\alpha-1/3)\beta\ bc}{}_{[k]\mu,\nu\square\pi(j),\xi} + [\tau^{(\alpha)\beta bc}{}_{[k]\mu,\nu,\xi}](Y^b{}_{[i]}+Y^c{}_{[j]}+Z)$

を生成する。

次に、全ての k=1,...,m、全ての β=1,...,λ、全ての h=2/3,1/3,0、全ての b,c,μ,v,ξ∈{0,1}に関して、

$\sigma'(\alpha-h)bc_{[k]\mu,\nu,\xi}$, $\tau'(\alpha-h)\beta bc_{[k]\mu,\nu,\xi}$,

を Z/qZ から一様無作為に選び,全ての k=1,...,m、全ての β=1,...,λ、全ての b,c,μ,v,ξ∈{0,1}に関して,

$A'(\alpha-2/3)bc_{[k]\pi(i),\mu,\nu,\xi}=A(\alpha-1)bc_{[k]\mu\square\pi(i),\nu,\xi}+[\sigma'(\alpha-2/3)bc_{[k]\mu,\nu,\xi}]G$

$B'(\alpha-2/3)bc_{[k]\pi(i):\mu,\nu,\xi}=B(\alpha-1)bc_{[k]\mu\square\pi(i),\nu,\xi}+[\sigma'(\alpha-2/3)bc_{[k]\mu,\nu,\xi}](Y^b_{[i]}+Y^c_{[j]}+Z)$

$C'(\alpha-2/3)\beta\ bc_{[k]\pi(i),\mu,\nu,\xi}=C(\alpha-1)\beta\ bc_{[k]\mu\square\pi(i),\nu\ \xi}+[\tau'(\alpha-2/3)\beta\ bc_{[k]\mu,\nu,\xi}]G$

$D'(\alpha-2/3)\beta\ bc_{[k]\pi(i),\mu,\nu,\xi}=D(\alpha-1)\beta\ bc_{[k]\mu\square\pi(i),\nu,\xi}+[\tau'(\alpha-2/3)\beta\ bc_{[k]\mu,\nu,\xi}](Y^b_{[i]}+Y^c_{[j]}+Z)$

$A'(\alpha-1/3)bc_{[k]\pi(j)\mu,\nu,\xi}=A(\alpha-2/3)bc_{[k]\mu,\nu\square\pi(j),\xi}+[\sigma'(\alpha-1/3)bc_{[k]\mu,\nu,\xi}]G$

$B'(\alpha-1/3)bc_{[k]\pi(j)\mu,\nu,\xi}=B(\alpha-2/3)bc_{[k]\mu,\nu\square\pi(j),\xi}+[\sigma'(\alpha-1/3)bc_{[k]\mu,\nu,\xi}](Y^b_{[i]}+Y^c_{[j]}+Z)$

$C'(\alpha-1/3)\beta\ bc_{[k]\pi(j)\mu,\nu,\xi}=C(\alpha-2/3)\beta\ bc_{[k]\mu,\nu\square\pi(j),\xi}+[\tau'(\alpha-1/3)\ \beta\ bc_{[k]\mu,\nu,\xi}]G$

$D'(\alpha-1/3)\beta\ bc_{[k]\pi(j)\mu,\nu,\xi}=D(\alpha-2/3)\beta\ bc_{[k]\mu,\nu\square\pi(j),\xi}+[\tau'(\alpha-1/3)\ \beta\ bc_{[k]\mu,\nu,\xi}](Y^b_{[i]}+Y^c_{[j]}+Z)$

$A'(\alpha)bc_{[k]\pi(k)\mu,\nu,\xi}=A(\alpha-1/3)bc_{[k]\mu,\nu\square\pi(j),\xi}+[\sigma'(\alpha)bc_{[k]\mu,\nu,\xi}]G$

$B'(\alpha)bc_{[k]\pi(k)\mu,\nu,\xi}=B(\alpha-1/3)bc_{[k]\mu,\nu\square\pi(j),\xi}+[\sigma'(\alpha)bc_{[k]\mu,\nu,\xi}](Y^b_{[i]}+Y^c_{[j]}+Z)$

$C'(\alpha)\beta\ bc_{[k]\pi(k)\mu,\nu,\xi}=C(\alpha-1/3)\beta\ bc_{[k]\mu,\nu\square\pi(j),\xi}+[\tau'(\alpha)\beta\ bc_{[k]\mu,\nu,\xi}]G$

$D'(\alpha)\beta\ bc_{[k]\pi(k)\mu nu\xi}=D(\alpha-1/3)\beta\ bc_{[k]\mu,\nu\square\pi(j),\xi}+[\tau'(\alpha)\ \beta\ bc_{[k]\mu,\nu,\xi}](Y^b_{[i]}+Y^c_{[j]}+Z)$

を生成する。

さらに全ての k=m+1,...,m+n、全ての β=1,...,λ、全てのb,ξ∈{0,1}に関して、

$s'^{(\alpha)b}_{[k]\xi}, t'^{(\alpha)b}_{[k]\xi}$

を Z/qZ から一様無作為に選び,全ての k=m+1,...,m+n,全ての $b,\xi \in \{0,1\}$ に関して、

$$A'^{(\alpha)b}_{[k]\pi(k),\xi} = A^{(\alpha-1)b}_{[k]\xi} \square \pi(k) + [s'^{(\alpha)b}_{[k]\xi}]G$$

$$B'^{(\alpha)b}_{[k]\pi(k),\xi} = B^{(\alpha-1)b}_{[k]\xi} \square \pi(k) + [s'^{(\alpha)b}_{[k]\xi}](Y^{b}_{[k]}+Z)$$

$$C'^{(\alpha)\beta b}_{[k]\pi(k)\xi} = C^{(\alpha-1)\beta b}_{[k]\xi} \square \pi(k) + [t'^{(\alpha)\beta b}_{[k]\xi}]G$$

$$D'^{(\alpha)\beta b}_{[k]\pi(k)\xi} = D^{(\alpha-1)\beta b}_{[k]\xi} \square \pi(k) + [t'^{(\alpha)\beta b}_{[k]\xi}](Y^{b}_{[k]}+Z)$$

を生成する。さらに全ての k=1,...,l,全ての $b,\xi \in \{0,1\}$ に関して、

$$s^{\dagger\prime(\alpha)b}_{[k]\xi},$$

を Z/qZ から一様無作為に選び、全ての k=1,...,l,全ての $b,\xi \in \{0,1\}$ に関して、

$$A^{\dagger\prime(\alpha)b}_{[k]\pi(k)\xi} = A^{\dagger(\alpha-1)b}_{[k]\xi} \square \pi(k) + [s^{\dagger\prime(\alpha)b}_{[k]\xi}]G$$

$$B^{\dagger\prime(\alpha)b}_{[k]\pi(k)\xi} = B^{\dagger(\alpha-1)b}_{[k]\xi} \square \pi(k) + [s^{\dagger\prime(\alpha)b}_{[k]\xi}](Y^{b}_{[k]}+Z)$$

を生成する。

次に、全ての k=1,...,m、全ての h=2/3,1/3,0 に関して、

$$\theta^{(\alpha)}_{[k]\pi(i)\square 1},$$

を Z/qZ から一様無作為に選ぶ。

次に、全ての k=1,...,m、全ての β=1,...,λ、全ての $b,c,\mu,\nu,\xi \in \{0,1\}$ に関して、

$\sigma''^{(\alpha-2/3)bc}{}_{[k]}\ \pi(i)\square 1,\mu,\nu,\xi$, $\sigma''^{(\alpha-1/3)bc}{}_{[k]}\ \pi(j)\square 1,\mu,\nu,\xi$, $\sigma''^{(\alpha)bc}{}_{[k]}$
$\pi(k)\square 1,\mu,\nu,\xi$, $\tau''^{(\alpha-2/3)\beta\ bc}{}_{[k]}\ \pi(i)\square 1,\mu,\nu,\xi$, $\tau''^{(\alpha-1/3)\beta\ bc}{}_{[k]}$
$\pi(j)\square 1,\mu,\nu,\xi$, $\tau''^{(\alpha)\beta bc}{}_{[k]}\ \pi(k)\square 1,\mu,\nu,\xi$

を Z/qZ から一様無作為に選ぶ。

次に、全ての k=m+1,...,m+n、全ての β=1,...,λ、全ての $b,\xi\in\{0,1\}$ に関して,

$s''^{(\alpha)b}{}_{[k]}\ \pi(k)\square 1,\xi$, $t''^{(\alpha)\beta b}{}_{[k]}\ \pi(k)\square 1,\xi$

を Z/qZ から一様無作為に選ぶ。次に、全ての k=1,...,l、全ての $b,\xi\in\{0,1\}$ に関して、

$s^{\dagger''^{(\alpha)b}}{}_{[k]}\ \pi(k)\square 1,\xi$, $t^{\dagger''^{(\alpha)b}}{}_{[k]}\ \pi(k)\square 1,\xi$

を Z/qZ から一様無作為に選ぶ。

次に、全ての k=1,...,m、全ての β=1,...,λ、全ての $b,c,\mu,\nu,\xi\in\{0,1\}$ に関して、

$A'^{(\alpha-2/3)bc}{}_{[k]}\ \pi(i)\square 1,\mu,\nu,\xi = [\sigma''^{(\alpha-2/3)bc}{}_{[k]}\ \pi(i)\square 1,\mu,\nu,\xi]G - [\theta^{(\alpha)}{}_{[k]}\pi(i)\square 1]\ A^{(\alpha-1)bc}{}_{[k]}\ \mu\square\pi(i),\nu,\xi$

$B'^{(\alpha-2/3)bc}{}_{[k]}\ \pi(i)\square 1,\mu,\nu,\xi = [\sigma''^{(\alpha-2/3)bc}{}_{[k]}\ \pi(i)\square 1,\mu,\nu,\xi]\ (Y^{b}{}_{[i]}+Y^{c}{}_{[j]}+Z) - [\theta^{(\alpha)}{}_{[k]}\pi(i)\square 1]\ B^{(\alpha-1)bc}{}_{[k]}\ \mu\square\pi(i),\nu,\xi$

$C'^{(\alpha-2/3)\beta\ bc}{}_{[k]}\ \pi(i)\square 1,\mu,\nu,\xi = [\tau''^{(\alpha-2/3)\beta\ bc}{}_{[k]}\ \pi(i)\square 1,\mu,\nu,\xi]G - [\theta^{(\alpha)}{}_{[k]}\pi(i)\square 1]\ C^{(\alpha-1)\beta\ bc}{}_{[k]}\ \mu\square\pi(i),\nu,\xi$

$D'^{(\alpha-2/3)\beta\ bc}{}_{[k]}\ \pi(i)\square 1,\mu,\nu,\xi = [\tau''^{(\alpha-2/3)\beta\ bc}{}_{[k]}\ \pi(i)\square 1,\mu,\nu,\xi]\ (Y^{b}{}_{[i]}+Y^{c}{}_{[j]}+Z) - [\theta^{(\alpha)}{}_{[k]}\pi(i)\square 1]\ D^{(\alpha-1)\beta\ bc}{}_{[k]}\ \mu\square\pi(i),\nu,\xi$

$A'^{(\alpha-1/3)bc}{}_{[k]}\ \pi(j)\square 1,\mu,\nu,\xi = [\sigma''^{(\alpha-1/3)bc}{}_{[k]}\ \pi(j)\square 1,\mu,\nu,\xi]G - [\theta^{(\alpha)}{}_{[k]}\pi(j)\square 1]\ A^{(\alpha-2/3)bc}{}_{[k]}\ \mu,\nu\square\pi(j),\xi$

$B'^{(\alpha-1/3)bc}{}_{[k]}\ \pi(j)\square 1,\mu,\nu,\xi = [\sigma''^{(\alpha-1/3)bc}{}_{[k]}\ \pi(j)\square 1,\mu,\nu,\xi]\ (Y^{b}{}_{[i]}+Y^{c}{}_{[j]}+Z) - [\theta^{(\alpha)}{}_{[k]}\pi(j)\square 1]\ B^{(\alpha-2/3)bc}{}_{[k]}\ \mu,\nu\square\pi(j),\xi$

$C'^{(\alpha-1/3)\beta\ bc}{}_{[k]}\ \pi(j)\square 1,\mu,\nu,\xi = [\tau''^{(\alpha-1/3)\beta\ bc}{}_{[k]}\ \pi(j)\square 1,\mu,\nu,\xi]G - [\theta^{(\alpha)}{}_{[k]}\pi(j)\square 1]\ C^{(\alpha-2/3)\beta\ bc}{}_{[k]}\ \mu,\nu\square\pi(j),\xi$

$D'^{(\alpha-1/3)\beta\ bc}{}_{[k]}\ \pi(j)\square 1,\mu,\nu,\xi = [\tau''^{(\alpha-1/3)\beta\ bc}{}_{[k]}\ \pi(j)\square 1,\mu,\nu,\xi]\ (Y^{b}{}_{[i]}+Y^{c}{}_{[j]}+Z) - [\theta^{(\alpha)}{}_{[k]}\pi(j)\square 1]\ D^{(\alpha-2/3)\beta\ bc}{}_{[k]}\ \mu,\nu\square\pi(j),\xi$

$A'^{(\alpha)bc}{}_{[k]}\ \pi(k)\square 1,\mu,\nu,\xi = [\sigma''^{(\alpha)bc}{}_{[k]}\ \pi(k)\square 1,\mu,\nu,\xi]G - [\theta^{(\alpha)}{}_{[k]}\pi(k)\square 1]\ A^{(\alpha-1/3)bc}{}_{[k]}\ \mu,\nu,\xi\square\pi(k)$

$B'^{(\alpha)bc}{}_{[k]}\ \pi(k)\square 1,\mu,\nu,\xi = [\sigma''^{(\alpha)bc}{}_{[k]}\ \pi(k)\square 1,\mu,\nu,\xi]\ (Y^{b}{}_{[i]}+Y^{c}{}_{[j]}+Z) - [\theta^{(\alpha)}{}_{[k]}\pi(k)\square 1]\ B^{(\alpha-1/3)bc}{}_{[k]}\ \mu,\nu,\xi\square\pi(k)$

$C'^{(\alpha)\beta\,bc}{}_{[k]}\ \pi(k)\square 1,\mu,\nu,\xi = [\tau''^{(\alpha)\beta\,bc}{}_{[k]}\ \pi(k)\square 1,\mu,\nu,\xi]G - [\theta^{(\alpha)}{}_{[k]}\pi(k)\square 1]\ C^{(\alpha-1/3)\beta\ bc}{}_{[k]}\ \mu,\nu,\xi\square\pi(k)$

$D'^{(\alpha)\beta\,bc}{}_{[k]}\ \pi(k)\square 1,\mu,\nu,\xi = [\tau''^{(\alpha)\beta\,bc}{}_{[k]}\ \pi(k)\square 1,\mu,\nu,\xi]\ (Y^{b}{}_{[i]}+Y^{c}{}_{[j]}+Z) - [\theta^{(\alpha)}{}_{[k]}\pi(k)\square 1]\ D^{(\alpha-1/3)\beta\ bc}{}_{[k]}\ \mu,\nu,\xi\square\pi(k)$

を生成する。

次に、全ての k=m+1,...,m+n、全ての β=1,...,λ、全ての $^{b,\xi\in\{0,1\}}$ に関して、

$A'^{(\alpha)b_{[k]}}{}_{\pi(i)\square 1,\xi} = [s''^{(\alpha-1)b_{[k]}}{}_{\pi(i)\square 1,\xi}]G - [\theta^{(\alpha)}{}_{[k]\pi(i)\square 1}]\, A^{(\alpha-1)b_{[k]}}{}_{\xi\square\pi(i)}$

$B'^{(\alpha)b_{[k]}}{}_{\pi(i)\square 1,\xi} = [s''^{(\alpha-1)b_{[k]}}{}_{\pi(i)\square 1,\xi}](Y^{\sim b_{[k]}} + Z) - [\theta^{(\alpha)}{}_{[k]\pi(i)\square 1}]\, B^{(\alpha-1)b_{[k]}}{}_{\xi\square\pi(i)}$

$C'^{(\alpha)\beta b_{[k]}}{}_{\pi(i)\square 1,\xi} = [t''^{(\alpha-1)\beta b_{[k]}}{}_{\pi(i)\square 1,\xi}]G - [\theta^{(\alpha)}{}_{[k]\pi(i)\square 1}]\, C^{(\alpha-1)\beta b_{[k]}}{}_{\xi\square\pi(i)}$

$D'^{(\alpha)\beta b_{[k]}}{}_{\pi(i)\square 1,\xi} = [t''^{(\alpha-1)\beta b_{[k]}}{}_{\pi(i)\square 1,\xi}](Y^{\sim b_{[k]}} + Z) - [\theta^{(\alpha)}{}_{[k]\pi(i)\square 1}]\, D^{(\alpha-1)\beta b_{[k]}}{}_{\xi\square\pi(i)}$

を生成する。

次に、全ての k=1,...,l、全ての $b,\xi \in \{0,1\}$ に関して、

$A^{\dagger'(\alpha)b_{[k]}}{}_{\pi(i)\square 1,\xi} = [s^{\dagger''(\alpha-1)b_{[k]}}{}_{\pi(i)\square 1,\xi}]G - [\theta^{(\alpha)}{}_{[k]\pi(i)\square 1}]\, A^{\dagger(\alpha-1)b_{[k]}}{}_{\xi\square\pi(i)}$

$B^{\dagger'(\alpha)b_{[k]}}{}_{\pi(i)\square 1,\xi} = [s^{\dagger''(\alpha-1)b_{[k]}}{}_{\pi(i)\square 1,\xi}](Y^{b_{[k]}} + Z) - [\theta^{(\alpha)}{}_{[k]\pi(i)\square 1}]\, B^{\dagger(\alpha-1)b_{[k]}}{}_{\xi\square\pi(i)}$

を生成する。

次に、

$S = \{ E,G,$

$\{$

$A^{(\alpha-h)bc}{}_{[k]\mu,\nu,\xi}, B^{(\alpha-h)bc}{}_{[k]\mu,\nu,\xi}, C^{(\alpha-h)\beta bc}{}_{[k]\mu,\nu,\xi}, D^{(\alpha-h)\beta bc}{}_{[k]\mu,\nu,\xi},$

$A'^{(\alpha-h)bc}{}_{[k]\zeta,\mu,\nu,\xi}, B'^{(\alpha-h)bc}{}_{[k]\zeta,\mu,\nu,\xi}, C'^{(\alpha-h)\beta bc}{}_{[k]\zeta,\mu,\nu,\xi}, D'^{(\alpha-h)\beta bc}{}_{[k]\zeta,\mu,\nu,\xi}$

$k=1,...,m;h=2/3,1/3,0;\beta=1,...,\lambda; b,c,\mu,\nu,\xi,\zeta \in \{0,1\}$

$\{$

$A^{(\alpha)b}{}_{[k]\xi}, B^{(\alpha)b}{}_{[k]\xi}, C^{(\alpha)\beta b}{}_{[k]\xi}, D^{(\alpha)\beta b}{}_{[k]\xi},$

$A'^{(\alpha)b}{}_{[k]\zeta,\xi}, B'^{(\alpha)b}{}_{[k]\zeta,\xi}, C'^{(\alpha)\beta b}{}_{[k]\zeta,\xi}, D'^{(\alpha)\beta b}{}_{[k]\zeta,\xi}$

$k=m+1,...,m+n;\beta=1,...,\lambda; b,\xi,\zeta \in \{0,1\}^l \}$

$\{$

$A^{\dagger(\alpha)b}{}_{[k]\xi}, B^{\dagger(\alpha)b}{}_{[k]\xi}$

$A^{\dagger'(\alpha)b}{}_{[k]\zeta,\xi}, B^{\dagger'(\alpha)b}{}_{[k]\zeta,\xi}$

$k=1,...,l; b,\xi,\zeta \in \{0,1\}^l \}$

を生成する。

次に、各 uα は、全ての k=1,...,m+n に関して

$$\theta^{(\alpha)}{}_{[k]} = \mathrm{Hash}(E,G,k,S)$$

を生成する。

次に、全ての k=1,...,m+n に関して

$$\theta^{(\alpha)}{}_{[k]\pi(i)} = \theta^{(\alpha)}{}_{[k]} - \theta^{(\alpha)}{}_{[k]\pi(i)-1}$$

を生成する。次に、全ての k=1,...,m、全ての β=1,...,λ、全ての h=2/3,1/3,0、全ての $b,c,\mu,\nu,\xi \in \{0,1\}$ に関して、

$$\sigma^{\prime\prime(\alpha-h)bc}{}_{[k]\pi(i),\mu,\nu,\xi} = \theta(\alpha)_{[k]\pi(i)}\,\sigma^{(\alpha-2/3)bc}{}_{[k]\mu,\nu,\xi} + \sigma^{\prime(\alpha-2/3)bc}{}_{[k]\mu,\nu,\xi} \bmod q$$

$$\tau^{\prime\prime(\alpha-h)\beta\,bc}{}_{[k]\pi(i),\mu,\nu,\xi} = \theta(\alpha)_{[k]\pi(i)}\,\tau^{(\alpha-2/3)\beta\ bc}{}_{[k]\mu,\nu,\xi} + \tau^{\prime(\alpha-2/3)\beta\ bc}{}_{[k]\mu,\nu,\xi} \bmod q$$

を生成する。

次に、全ての k=m+1,...,m+n、全ての β=1,...,λ、全ての $b,\xi \in \{0,1\}$ に関して,

$$s^{\prime\prime(\alpha)b}{}_{[k]\pi(i)\xi} = \theta(\alpha)_{[k]\pi(i)}\,s^{(\alpha-1)b}{}_{[k]\xi} + s^{\prime(\alpha-1)b}{}_{[k]\xi} \bmod q$$

$$t^{\prime\prime(\alpha)\beta\,b}{}_{[k]\pi(i)\xi} = \theta(\alpha)_{[k]\pi(i)}\,t^{(\alpha-1)\beta\,b}{}_{[k]\xi} + t^{\prime(\alpha-1)b}{}_{[k]\xi} \bmod q$$

を生成する。

次に、全ての k=1,...,l、全ての $b,\xi \in \{0,1\}$ に関して,

$$s\dagger^{\prime\prime(\alpha)b}{}_{[k]\pi(i)\xi} = \theta(\alpha)_{[k]\pi(i)}\,s\dagger^{(\alpha-1)b}{}_{[k]\xi} + s\dagger^{\prime(\alpha-1)b}{}_{[k]\xi} \bmod q$$

を生成する。

最後に、全ての

$$k=1,...,m;h=2/3,1/3,0;\beta=1,...,\lambda;b,c,\mu,\nu,\xi,\zeta \in \{0,1\}$$

に関する

$A^{(\alpha-h)bc}{}_{[k]\mu,\nu,\xi}$, $B^{(\alpha-h)bc}{}_{[k]\mu,\nu,\xi}$, $C^{(\alpha-h)\beta bc}{}_{[k]\mu,\nu,\xi}$, $D^{(\alpha-h)\beta bc}{}_{[k]\mu,\nu,\xi}$,

$A'^{(\alpha-h)bc}{}_{[k]\zeta,\mu,\nu,\xi}$, $B'^{(\alpha-h)bc}{}_{[k]\zeta,\mu,\nu,\xi}$, $C'^{(\alpha-h)\beta bc}{}_{[k]\zeta,\mu,\nu,\xi}$, $D'^{(\alpha-h)\beta bc}{}_{[k]\zeta,\mu,\nu,\xi}$,

$\sigma''^{(\alpha)b}{}_{[k]\zeta,\xi}$, $\tau''^{(\alpha)\beta b}{}_{[k]\zeta,\xi}$,

及び、全ての

$$k=m+1,\ldots,m+n;\beta=1,\ldots,\lambda;b,\xi,\zeta\in\{0,1\}$$

に関する

$A^{(\alpha)b}{}_{[k]\xi}$, $B^{(\alpha)b}{}_{[k]\xi}$, $C^{(\alpha)\beta b}{}_{[k]\xi}$, $D^{(\alpha)\beta b}{}_{[k]\xi}$,

$A'^{(\alpha)b}{}_{[k]\zeta,\xi}$, $B'^{(\alpha)b}{}_{[k]\zeta,\xi}$, $C'^{(\alpha)\beta b}{}_{[k]\zeta,\xi}$, $D'^{(\alpha)\beta b}{}_{[k]\zeta,\xi}$,

$s''^{(\alpha-h)bc}{}_{[k]\zeta,\mu,\nu,\xi}$, $t''^{(\alpha-h)\beta bc}{}_{[k]\zeta,\mu,\nu,\xi}$,

及び、全ての

$$k=1,\ldots,l;b,\xi,\zeta\in\{0,1\}$$

に関する

$A^{\dagger(\alpha)b}{}_{[k]\xi}$, $B^{\dagger(\alpha)b}{}_{[k]\xi}$,

$A^{\dagger'(\alpha)b}{}_{[k]\zeta,\xi}$, $B^{\dagger'(\alpha)b}{}_{[k]\zeta,\xi}$,

$s^{\dagger''(\alpha-h)bc}{}_{[k]\zeta,\mu,\nu,\xi}$,

及び, 全てのk=1,....,m+n に関する

$\theta^{(\alpha)}{}_{[k]\zeta}$

を証明とする。上記証明の検証方法は以下の通り。

検証者は、

S = [E,G,

[

$A^{(\alpha-h)bc}{}_{[k]\mu,\nu,\xi}$, $B^{(\alpha-h)bc}{}_{[k]\mu,\nu,\xi}$, $C^{(\alpha-h)\beta bc}{}_{[k]\mu,\nu,\xi}$, $D^{(\alpha-h)\beta bc}{}_{[k]\mu,\nu,\xi}$,

$A'^{(\alpha-h)bc}{}_{[k]\zeta,\mu,\nu,\xi}$, $B'^{(\alpha-h)bc}{}_{[k]\zeta,\mu,\nu,\xi}$, $C'^{(\alpha-h)\beta bc}{}_{[k]\zeta,\mu,\nu,\xi}$, $D'^{(\alpha-h)\beta bc}{}_{[k]\zeta,\mu,\nu,\xi}$

]$_{k=1,...,m;h=2/3,1/3,0;\beta=1,...,\lambda;\ b,c,\mu,\nu,\xi,\zeta\in\{0,1\}}$

[

$A^{(\alpha)b}{}_{[k]\xi}$, $B^{(\alpha)b}{}_{[k]\xi}$, $C^{(\alpha)\beta b}{}_{[k]\xi}$, $D^{(\alpha)\beta b}{}_{[k]\xi}$,

$A'^{(\alpha)b}{}_{[k]\zeta,\xi}$, $B'^{(\alpha)b}{}_{[k]\zeta,\xi}$, $C'^{(\alpha)\beta b}{}_{[k]\zeta,\xi}$, $D'^{(\alpha)\beta b}{}_{[k]\zeta,\xi}$

]$_{k=m+1,...,m+n;\beta=1,...,\lambda;b,\xi,\zeta\in\{0,1\}}$]

[

$A^{\dagger(\alpha)b}{}_{[k]\xi}$, $B^{\dagger(\alpha)b}{}_{[k]\xi}$

$A^{\dagger'(\alpha)b}{}_{[k]\zeta,\xi}$, $B^{\dagger'(\alpha)b}{}_{[k]\zeta,\xi}$

]$_{k=1,...,l;b,\xi,\zeta\in\{0,1\}}$]

を生成し、各 uα は、全ての k=1,...,m+n に関して

$$\theta^{(\alpha)}{}_{[k]} = \mathrm{Hash}(E,G,k,S)$$

を生成し、全ての k=1,...,m に関して、

$$\theta^{(\alpha)}{}_{[k]0} + \theta^{(\alpha)}{}_{[k]1} = \theta^{(\alpha)}{}_{[k]}$$

が成り立つことを確認する。検証者は次に、

$$k=1,\ldots,m;h=2/3,1/3,0;\beta=1,\ldots,\lambda;b,c,\mu,\nu,\xi,\zeta\in[0,1]$$

に関して

$$[\sigma''(\alpha-2/3)bc_{[k]}\xi,\mu,\nu,\xi]G=[\theta(\alpha)_{[k]}\xi](A(\alpha-2/3)bc_{[k]}\mu,\nu,\xi-A(\alpha-1)bc_{[k]}\mu\square\xi,\nu,\xi)-A'(\alpha-2/3)bc_{[k]}\xi,\mu,\nu,\xi$$

$$[\sigma''(\alpha-2/3)bc_{[k]}\xi,\mu,\nu,\xi](Y^b_{[i]}+Y^c_{[j]}+Z)=[\theta(\alpha)_{[k]}\xi](B(\alpha-2/3)bc_{[k]}\mu,\nu,\xi-B(\alpha-1)bc_{[k]}\mu\square\xi,\nu,\xi)-B'(\alpha-2/3)bc_{[k]}\xi,\mu,\nu,\xi$$

$$[\tau''(\alpha-2/3)\beta\ bc_{[k]}\xi,\mu,\nu,\xi]G=[\theta(\alpha)_{[k]}\xi](C(\alpha-2/3)\beta\ bc_{[k]}\mu,\nu,\xi-C(\alpha-1)\beta\,bc_{[k]}\mu\square\xi,\nu,\xi)-C'(\alpha-2/3)\beta\ bc_{[k]}\xi,\mu,\nu,\xi$$

$$[\tau''(\alpha-2/3)\beta\ bc_{[k]}\xi,\mu,\nu,\xi](Y^b_{[i]}+Y^c_{[j]}+Z)=[\theta(\alpha)_{[k]}\xi](D(\alpha-2/3)\beta\ bc_{[k]}\mu,\nu,\xi-D(\alpha-1)\beta\,bc_{[k]}\mu\square\xi,\nu,\xi)-D'(\alpha-2/3)\beta\ bc_{[k]}\xi,\mu,\nu,\xi$$

$$[\sigma''(\alpha-1/3)bc_{[k]}\xi,\mu,\nu,\xi]G=[\theta(\alpha)_{[k]}\xi](A(\alpha-1/3)bc_{[k]}\mu,\nu,\xi-A(\alpha-2/3)bc_{[k]}\mu\square\xi,\nu,\xi)-A'(\alpha-1/3)bc_{[k]}\xi,\mu,\nu,\xi$$

$$[\sigma''(\alpha-1/3)bc_{[k]}\xi,\mu,\nu,\xi](Y^b_{[i]}+Y^c_{[j]}+Z)=[\theta(\alpha)_{[k]}\xi](B(\alpha-2/3)bc_{[k]}\mu,\nu,\xi-B(\alpha-2/3)bc_{[k]}\mu\square\xi,\nu,\xi)-B'(\alpha-1/3)bc_{[k]}\xi,\mu,\nu,\xi$$

$$[\tau''(\alpha-1/3)\beta\ bc_{[k]}\xi,\mu,\nu,\xi]G=[\theta(\alpha)_{[k]}\xi](C(\alpha-1/3)\beta\ bc_{[k]}\mu,\nu,\xi-C(\alpha-2/3)\beta\ bc_{[k]}\mu\square\xi,\nu,\xi)-C'(\alpha-1/3)\beta\ bc_{[k]}\xi,\mu,\nu,\xi$$

$$[\tau''(\alpha-1/3)\beta\ bc_{[k]}\xi,\mu,\nu,\xi](Y^b_{[i]}+Y^c_{[j]}+Z)=[\theta(\alpha)_{[k]}\xi](D(\alpha-1/3)\beta\ bc_{[k]}\mu,\nu,\xi-D(\alpha-2/3)\beta\ bc_{[k]}\mu\square\xi,\nu,\xi)-D'(\alpha-1/3)\beta\ bc_{[k]}\xi,\mu,\nu,\xi$$

$$[\sigma''(\alpha)bc_{[k]}\xi,\mu,\nu,\xi]G=[\theta(\alpha)_{[k]}\xi](A(\alpha)bc_{[k]}\mu,\nu,\xi-A(\alpha-1/3)bc_{[k]}\mu\square\xi,\nu,\xi)-A'(\alpha)bc_{[k]}\xi,\mu,\nu,\xi$$

$$[\sigma''(\alpha)bc_{[k]}\xi,\mu,\nu,\xi](Y^b_{[i]}+Y^c_{[j]}+Z)=[\theta(\alpha)_{[k]}\xi](B(\alpha-1/3)bc_{[k]}\mu,\nu,\xi-B(\alpha-2/3)bc_{[k]}\mu\square\xi,\nu,\xi)-B'(\alpha)bc_{[k]}\xi,\mu,\nu,\xi$$

$$[\tau''(\alpha)\beta\,bc_{[k]}\xi,\mu,\nu,\xi]G=[\theta(\alpha)_{[k]}\xi](C(\alpha)\beta\,bc_{[k]}\mu,\nu,\xi-C(\alpha-1/3)\beta\ bc_{[k]}\mu\square\xi,\nu,\xi)-C'(\alpha)\beta\,bc_{[k]}\xi,\mu,\nu,\xi$$

$$[\tau''(\alpha)\beta\,bc_{[k]}\xi,\mu,\nu,\xi](Y^b_{[i]}+Y^c_{[j]}+Z)=[\theta(\alpha)_{[k]}\xi](D(\alpha)\beta\,bc_{[k]}\mu,\nu,\xi-D(\alpha-1/3)\beta\ bc_{[k]}\mu\square\xi,\nu,\xi)-D'(\alpha)\beta\,bc_{[k]}\xi,\mu,\nu,\xi$$

が成り立つことを確認する。

検証者は次に、

$k=m+1,\ldots,m+n;\beta=1,\ldots,\lambda;b,\xi,\zeta\in\{0,1\}$

に関して

$$[s''(\alpha)b_{[k]\zeta,\xi}]G=[\theta(\alpha)_{[k]\zeta}](A(\alpha)b_{[k]\xi}-A(\alpha-1)b_{[k]\xi\Box\zeta})-A'(\alpha)b_{[k]\zeta,\xi}$$

$$[s''(\alpha)b_{[k]\zeta,\xi}](Y\tilde{}b_{[k]}+Z)=[\theta(\alpha)_{[k]\zeta}](B(\alpha)b_{[k]\xi}-B(\alpha-1)b_{[k]\xi\Box\zeta})-B'(\alpha)b_{[k]\zeta,\xi}$$

$$[t''(\alpha)\beta b_{[k]\zeta,\xi}]G=[\theta(\alpha)_{[k]\zeta}](C(\alpha)\beta b_{[k]\xi}-C(\alpha-1)\beta b_{[k]\xi\Box\zeta})-C'(\alpha)\beta b_{[k]\zeta,\xi}$$

$$[t''(\alpha)\beta b_{[k]\zeta,\xi}](Y\tilde{}b_{[k]}+Z)=[\theta(\alpha)_{[k]\zeta}](D(\alpha)\beta b_{[k]\xi}-D(\alpha-1)\beta b_{[k]\xi\Box\zeta})-D'(\alpha)\beta b_{[k]\zeta,\xi}$$

が成り立つことを確認する。検証者は次に、

$k=1,\ldots,l;b,\xi,\zeta\in\{0,1\}$

に関して

$$[s\dagger''(\alpha)b_{[k]\zeta,\xi}]G=[\theta(\alpha)_{[k]\zeta}](A\dagger(\alpha)b_{[k]\xi}-A\dagger(\alpha-1)b_{[k]\xi\Box\zeta})-A\dagger'(\alpha)b_{[k]\zeta,\xi}$$

$$[s\dagger''(\alpha)b_{[k]\zeta,\xi}](Yb_{[k]}+Z)=[\theta(\alpha)_{[k]\zeta}](B\dagger(\alpha)b_{[k]\xi}-B\dagger(\alpha-1)b_{[k]\xi\Box\zeta})-B'(\alpha)b_{[k]\zeta,\xi}$$

が成り立つことを確認する。

[別記述 F]

証明者(計算者) u_α は, 全ての$k=1,\ldots,m+n$, 全ての$b,c\in\{0,1\}$ に関して、

全ての証明者(計算者) $\{u_\alpha\}_{\alpha=1,\ldots,\lambda}$ は、 $z'(\alpha)\in_R Z/qZ$ を一様無作為に生成し, $Z'(\alpha)=[z'(\alpha)]G$ を生成し、全ての k=1,...,m、全ての $b,c\in\{0,1\}$ 、全ての β=1,...,λ に関して

$$A'(\lambda)\alpha bc_{[k]000} = [z'(\alpha)]A(\lambda)bc_{[k]000}$$

$$C'(\lambda)\alpha\beta bc_{[k]000} = [z'(\alpha)]C(\lambda)\alpha bc_{[k]000}$$

を生成し、全ての k=m+1,...,m+n、全ての $b \in [0,1]$ 、全ての β=1,...,λ に関して

$$A'(\lambda)\alpha b_{[k]0} = [z'(\alpha)]A(\lambda)b_{[k]0}$$

$$C'(\lambda)\alpha\beta b_{[k]0} = [z'(\alpha)]C(\lambda)\alpha b_{[k]0}$$

を生成し、全ての k=1,...,l、全ての $b \in [0,1]$ に関して

$$A\dagger'(\lambda)\alpha b_{[k]0} = [z'(\alpha)]A\dagger(\lambda)b_{[k]0}$$

を生成する。

$$S = \{ \{ A^{(\lambda)bc}_{[k]000}, C^{(\lambda)\beta bc}_{[k]000}, \}_{k=1,...,m;b,c=0,1;\beta=1,...,\lambda},$$

$$\{ A^{(\lambda)b}_{[k]0}, C^{(\lambda)\beta b}_{[k]0} \}_{k=m+1,...,m+n;b=0,1;\beta=1,...,\lambda},$$

$$\{ A^{\dagger(\lambda)b}_{[k]0} \}_{k=1,...,l;b=0,1},$$

$$\{ A^{\sharp(\lambda)\alpha bc}_{[k]000}, C^{\sharp(\lambda)\alpha\beta bc}_{[k]000} \}_{k=1,...,m;b,c=0,1;\beta=1,...,\lambda},$$

$$\{ A^{\sharp(\lambda)\alpha b}_{[k]0}, C^{\sharp(\lambda)\alpha \text{ beta } b}_{[k]0} k=m+1,...,m+n;b=0,1;\beta=1,...,\lambda,$$

$$\{ A^{\dagger\sharp(\lambda)\alpha b}_{[k]0} \}_{k=1,...,l;b=0,1},$$

$$\{z'(\alpha)\},$$

$$\{ A'^{(\lambda)\alpha bc}_{[k]000}, C'^{(\lambda)\alpha\beta bc}_{[k]000} \}_{k=1,...,m;b,c=0,1;\beta=1,...,\lambda},$$

$$\{ A'^{(\lambda)\alpha b}_{[k]0}, C'^{(\lambda)\alpha\beta b}_{[k]0} \}_{k=m+1,...,m+n;b=0,1;\beta=1,...,\lambda},$$

$$\{ A^{\dagger'(\lambda)\alpha b}_{[k]0} \}_{k=1,...,l;b=0,1}, \} \}$$

を生成し、さらに

$$\theta = \text{Hash}(E,G,S) \bmod q$$

を生成する。さらに

$$z''(\alpha) = z(\alpha)\theta + z'(\alpha) \bmod q$$

を生成する。証明者は、

$Z'(\alpha)$, $\{A'(\lambda)^{\alpha bc}_{[k]000}, C'(\lambda)^{\alpha\beta bc}_{[k]000}\}_{k=1,...,m;b,c=0,1;\beta=1,...,\lambda}$,

$\{A'(\lambda)^{\alpha b}_{[k]0}, C'(\lambda)^{\alpha\beta b}_{[k]0}\}_{k=m+1,...,m+n;b=0,1;\beta=1,...,\lambda}$,

$\{A\dagger'(\lambda)^{\alpha b}_{[k]0}\}_{k=1,...,l;b=0,1}$,

$z''(\alpha)$

を証明とする。上記証明の検証方法は以下の通り。

検証者は、

$S = [\{A(\lambda)^{bc}_{[k]000}, C(\lambda)^{\beta bc}_{[k]000},\}_{k=1,...,m;b,c=0,1;\beta=1,...,\lambda}$,

$\{A(\lambda)^{b}_{[k]0}, C(\lambda)^{\beta b}_{[k]0}\}_{k=m+1,...,m+n;b=0,1;\beta=1,...,\lambda}$,

$\{A\dagger(\lambda)^{b}_{[k]0}\}_{k=1,...,l;b=0,1}$,

$\{A\sharp(\lambda)^{\alpha bc}_{[k]000}, C\sharp(\lambda)^{\alpha\beta bc}_{[k]000}\}_{k=1,...,m;b,c=0,1;\beta=1,...,\lambda}$,

$\{A\sharp(\lambda)^{\alpha b}_{[k]0}, C\sharp(\lambda)^{\alpha\beta b}_{[k]0}\}_{k=m+1,...,m+n;b=0,1;\beta=1,...,\lambda}$,

$\{A\dagger\sharp(\lambda)^{\alpha b}_{[k]0}\}_{k=1,...,l;b=0,1}$,

$[Z'(\alpha)]$,

$\{A'(\lambda)^{\alpha bc}_{[k]000}, C'(\lambda)^{\alpha\beta bc}_{[k]000}\}_{k=1,...,m;b,c=0,1;\beta=1,...,\lambda}$,

$\{A'(\lambda)^{\alpha b}_{[k]0}, C'(\lambda)^{\alpha\beta b}_{[k]0}\}_{k=m+1,...,m+n;b=0,1;\beta=1,...,\lambda}$,

$\{A\dagger'(\lambda)^{\alpha b}_{[k]0}\}_{k=1,...,l;b=0,1}, \}]$

を生成し、さらに

$$\theta = \mathrm{Hash}(E,G,S) \bmod q$$

を計算して、

$$[z''(\alpha)]G = Z'(\alpha) + [\theta]Z(\alpha)$$

全ての

$$k=1,\ldots,m,\ b,c \in [0,1],\ \beta=1,\ldots,\lambda$$

に関して

$$[z''(\alpha)]\,A(\lambda)bc_{[k]000} = A'(\lambda)\alpha bc_{[k]000} + [\theta]\,A\sharp(\lambda)\alpha bc_{[k]000}$$

$$[z''(\alpha)]C(\lambda)\beta bc_{[k]000} = C'(\lambda)\alpha\beta bc_{[k]000} + [\theta]C\sharp(\lambda)\alpha\beta bc_{[k]000}$$

全ての

$$k=m+1,\ldots,m+n,\ b\in [0,1],\ \beta=1,\ldots,\lambda$$

に関して

$$[z''(\alpha)]A(\lambda)b_{[k]0} = A'(\lambda)\alpha b_{[k]0} + [\theta]A\sharp(\lambda)\alpha b_{[k]0}$$

$$[z''(\alpha)]C(\lambda)\beta b_{[k]0} = C'(\lambda)\alpha\beta b_{[k]0} + [\theta]C\sharp(\lambda)\alpha\beta b_{[k]0}$$

全ての $k=1,\ldots,l,\ b\in[0,1]$ に関して

$$[z''(\alpha)]A\dagger(\lambda)b_{[k]0} = A\dagger'(\lambda)\alpha b_{[k]0} + [\theta]A\dagger\sharp(\lambda)\alpha b_{[k]0}$$

を確認する。

[別記述 G]

計算者 $u(\alpha)$ は $z'(\alpha) \in_R Z/qZ$ を一様無作為に生成し、全ての k=1,...,l に関

して,

$$A^{\dagger'}_{[k]} = [z'(\alpha)]A^{\dagger b\lceil k\rfloor}_{[k]}$$

を生成する。証明者は、

$$S = \{ \{ A^{\dagger b\lceil k\rfloor}_{[k]} \}_{k=1,\ldots,l},$$

$$\{ A^{\dagger\sharp}_{[k]} \}_{k=1,\ldots,l},$$

$$\{ A^{\dagger'}_{[k]} \}_{k=1,\ldots,l} \}$$

を生成して、

$$\theta = \mathrm{Hash}(E, G, S) \bmod q$$

を生成する。証明者は

$$z''(\alpha) = \theta\, z(\alpha) + z'(\alpha) \bmod q$$

を生成する。証明者

$$\{ A^{\dagger\sharp}_{[k]} \}_{k=1,\ldots,l}, z''(\alpha)$$

を証明とする。上記証明の検証方法は以下の通り。検証者は、

$$S = \{ \{ A^{\dagger b\lceil k\rfloor}_{[k]} \}_{k=1,\ldots,l},$$

$$\{ A^{\dagger\sharp}_{[k]} \}_{k=1,\ldots,l},$$

$$\{ A^{\dagger'}_{[k]} \}_{k=1,\ldots,l} \}$$

を生成して,

$$\theta = \mathrm{Hash}(E, G, S) \bmod q$$

を生成する。検証者は

$$[z''(\alpha)]A^{\dagger}b^{\lceil k \rfloor}{}_{[k]} = A^{\dagger'}{}_{[k]} + [\theta]\, A^{\dagger\dagger}{}_{[k]}$$

を確認できたら証明を受理する。

実施例２

本発明の第２の実施例について、図１４ないし図１８を用いて説明する。

本実施例においては、図１４に示すように計算装置 1401 が N 個あり、それぞれ計算装置 1403 を備えているものとする。以下ではこの計算機を順番に U1,...,UN と呼ぶことにする。記法の都合上、UN の事を U0 とも書く事にする。

［方式の概略］

［データの流れ］

実施例２におけるデータの流れを図１６を参照して説明する。

まず、計算装置 1401 の U1 は DATA00 を計算する。これを「0 周目の計算」とよぶ(1701)。

次に「一周目の計算」を行う。

U1 は $DATA_0^0$ から $DATA_1^1$ を計算して、DATA11 を U2 に送る(1711)。

次に U2 は DATA11 から $DATA_1^2$ を計算し、DATA12 を U3 に送る(1712)。

以下順にデータを送って行き、UN は $DATA1^{N-1}$ から $DATA_1^N$ を計算し、DATA1N を U1 に送る(1710)。ここまでが一周目の計算である。

次に「二周目の計算」を行う。

U1 は DATA1N から $DATA_2^1$ を計算して、DATA21 を U2 に送る(1721)。

次に U2 は DATA21 から $DATA_2^2$ を計算し、DATA21 を U3 に送る(1722)。

以下順にデータを送って行き、UN は $DATA_2^{N-1}$ から $DATA_2^N$ を計算し、DATA2N を U1 に送る(1720)。ここまでが二周目の計算である。

次に「三周目の計算」を行う。

U1 は DATA2N から $DATA_3^1$ を計算して、DATA21 を U2 に送る(1731)。

以下順にデータを送って行き、UN が $DATA_3^{N-1}$ から DATA3N を計算し終えたところでプロトコルが終了となる。

[各計算装置 1401 の入出力]

次に各計算装置 1401 のやり取りするデータの入出力を図 14 を参照して説明する。

各計算装置 1401 には、回路の情報 1404、および回路の部分入力 1402 が入力される。

ここでは、回路の情報 1404 が表す回路の入力素子以外の素子の fan-in の数が 2 である場合に対し説明する。

回路の入力素子 w への入力 bw は U1、...、UN のいずれかが秘密裡に所有しているものとする。U1 の事を UN+1 とも書く事にする。

Ul が秘密裡に所有している入力ビットの組が回路の部分入力 1402 である。

回路の情報 1404 が表す回路の入力素子 i を、いかなる入力が入っても bw を出力する素子だと思い直した回路を以下 C[1]と表す。

C[1]の全てのゲートの fan-in の数は 2 である。

素子 w の左下、右下の fan-in をそれぞれ L(w)、R(w)と書く事にする。

各計算装置 1401 に回路の情報 1404、および回路の部分入力 1402 が入力されたら、まず U1 は後で説明する手順に従って 0 周目の計算を行う。

1 周目、2 周目、3 周目の計算での入出力は同様のデータ構造を持っている。i=1,2,3 に対し、ユーザ Ul が第 i 周目の計算で Ul+1 に送信するデータを DATAil と表す事にする。DATAi-1N を DATAi0 とも書く事にする。

また、第 0 周目の計算で U1 が行った計算の計算結果を DATA01 と書く。

$DATA_i^l$ は、$DATA_i^l = DATA_i^{l-1} || BODY_i^l || PROOF_i^l || SIG_i^l$ という形をしている。

DATAil-1 は Ul-1 から送られてきたメッセージ、BODYil はメッセージの本体、PROOFil は BODYil の正当性証明文、SIGil は Ul の DATAil-1 || BODYil ||PROOFil に対する署名。

1 周目、2 周目、3 周目の計算の概略を説明する。

第 i 周目の計算において、Ul はまず DATAil-1 を Ul-1 から受け取る(1501)。

(一周目の U1 のみは例外的に自分で作ったデータ DATA01 を使う)。

$DATA_i^{l-1}$ を受け取ったら、Ul は正当性証明文 PROOF11、...,PROOFl-11 を全て検証する(1502)。そして次に Ul は署名文 SIG_i^1、...、SIGl-11 を全て検証する(1503)。

第 1 周目の場合で、しかも l=1 の場合のみ 1504 の計算を行う。次に Ul は乱数生成を行う(1505)。そして Ul はその乱数を用いて本計算を行い、BODYil を作成する(1506)。本計算を終えたら Ul は BODYil の正当性証明文 PROOFil を作成する(1507)。そして Ul は DATAil-1 || BODYil ||

PROOFil に対する署名文 SIGil を作成する(1508)。

最後に Ul は DATAil =DATAil-1 || BODYil || PROOFil ||SIGil を Ul+1 に送信する(1509)。

[記号]

以下に、本明細書で使用する記号の説明を行う。

[暗号方式 E[27]]

G[1]を、アーベル群で DDH 問題が難しいもの(例えば有限体上の楕円曲線群)とし、G[1]の位数を p とし、G[1]の零元を O と表す。

η を記号とし、以下の記号を定義する。ただし、

$$P[|0|] \in G[1]$$

に対し、(P[|0|],0)を略記して単に P[|0|]と表し、自然に

$$F_p \subset B[12],\ G[1] \subset G[12B]$$

とみなし、G[12B]上の和を成分毎の和により定義し、

$$W[12] = B12^{\kappa} \text{ とし、}$$
$$G[12W] = G[12B]^{\kappa} \text{ とする。}$$
$$w[2] \in W[12]$$

の α 成分を w[2|α|]と表し、W[12]上の和と積を成分毎の和と積により定義し、G[12W]上の和とスカラー倍を成分毎の和とスカラー倍により定義する。

- $B[12]=F_p[\eta]/(\eta^2-1)$,
- $\phi[24](1)=1$, $\phi[24](0)=\eta$,
- $G[12B]=G[1]^2$、
- $aP[2]=(a[|0|]P[|0|]+a[|1|]P[|1|], aa[|0|]Pa[|1|]+a[|1|]Pa[|0|])$
- $W[12]=B[12]^{\kappa}$、
- $e[|i|]=(0,\cdots,0,1,0,\cdots,0)$ （i番目のみが1）
- $\phi[2]: F_p \to W[12]$ を $x \to \Sigma_{\alpha}\ \phi[2](x[|\alpha|])e[|\alpha|]$
- ただしここで
  - $P[2]=(P[|0|],P[|1|])$, $P[23]=(P[3|0|],P[3|1|]) \in G[12B]$, $a=a[|0|]+a[|1|]\eta \in B[12]$、$P[2]=(P[|0|],P[|1|]) \in G[12B]$,
  - κ ：pのビット数,
  - $x=x[|k-1|] \,||\, \cdots \,||\, x[|0|]$,
  - $G[12W]=G[12B]^{\kappa}$,

暗号方式 E[27]は G[12W]における、楕円 ElGamal 暗号の類似物である。

秘密鍵空間を Fp、公開鍵空間を G[12W]2、平文空間を G[12W]、乱数空間を W[12]とする。

鍵生成をするには、$P=P[|0|]+\eta P[|1|]$で $P[|0|],P[|1|]\neq O$ となるものを任意に選ぶ。ランダムに $a \in F_p$ を選び、Q=aP とする。a が秘密鍵、(P,Q)が公開鍵である。平文 M を暗号化するには一様かつランダムに $r \in B[12]$ を選び、暗号文 (P[3],Q[3])=(rP,M+rQ)を計算する。(P[3],Q[3])を復号するには Q[3]-aP[3]を計算すれば良い。[暗号方式 E[2],E[25]]

以下を定義する：

- K[1]={ {x[|wWh|]}(w∈C[1],W∈{L,R},h∈{0,1}を走る) | x[|wWh|]∈F_r
- A[12]={ { a[2|wWijk|]} ({w∈C[1],W∈{L,R},i,j,k∈{0,1}}を走る)|a[
- A[125]={ { A[25|wWijk|i[6]j[6]k[6]]({w∈C[1],W∈{L,R},i,i[6],j,j[
  |A[25|wWijk|i[6]j[6]k[6]]∈W[12]}
- G[1|K|]={ {P[|wWh|]} ({w∈C[1],W∈{L,R},h∈{0,1}} を走る)|P[|wWh
- G[12|A|]={{P[2|wWijk|]}(w∈C[1],W∈{L,R},i,j,k∈{0,1}})|P[2|wWi
- G[124|A|]={ { P[24|wWijk|i[6]j[6]k[6]]}
  ({w∈C[1],W∈{L,R},i,j,k,i[6],j[6],k[6]∈{0,1}}を走る)
  |P[24|wWijk|i[6]j[6]k[6]]∈G[12W],
- aA=(aA[|1|],aA[|2|])
- a[5]A[5]=(a[5]A[5|1|],a[5]A[5|2|])
- ただしここで
  - a ∈A[12]
  - A=(a[|1|],A[|2|]) ∈ G[12|A|]^2
  - a[5] ∈ A[125]
  - A[5]=(A[5|1|],A[5|2|]) ∈ G[124|A|]^2

κ の元 x の wWh 成分を x[|wWh|]と書く事にし、A[12]の元 x[2]の wWijk 成分を x[|wWijk|] と書く事にし、A[125] の元 A[25] の wWijk,i[6],j[6]{},k[6] 成分を x[|wWijk|i[6]j[6]k[6]]と書く事にする。

多重配列の和と積、スカラー倍を、成分毎の和と積により定義する。ただし例外的に、A[125]の元同士の積、および G[124|A|]の元の A[125]の元によるスカラー倍のみは

- a[25]*b[25]=Σ i[7],j[7],k[7]
  a[25|wWijk|i[7]j[7]k[7]]
  b[25|wWi[7]j[7]k[7]|i[6]j[6]k[6]],
- a[25]*P[24]=Σ a[25|wWijk|i[7]j[7]k[7]]
  P[24|wWi[7] j[7] k[7]|i[7]j[7]k[7]]
  (i[7],j[7],k[7]に関する和)

により定義する。

以下の記号を定義する。

- E[25][(Z[2]|s[25])](M[25])
  =
  {E[27][(Z[2]|s[25|wWijk|i[6]j[6]k[6]])](M[25|wWijk|i[6]j[6]k[6]])}
- E[25][(Y[2]|s[25])](M[25])
  =
  E[25][(s[25]|Z[25])](M[25])
- E[2][(x[2]|r[2])](M[2])
  =
  {E[27][(x[2|wWijk|]|r[2|wWijk|])](M[2|wWijk|])
- E[2][(Y[2]|r[2])](M[2])
  =
  E[2][(x[2]|r[2])](M[2])

・ ただしここで

- M[25]={M[25|wWijk|i[6]j[6]k[6]]},
  M[25|wWijk|i[6]j[6]k[6]] ∈ G[12W]
- Z[2]={Z[25|wWijk|i[6]j[6]k[6]]},
  (Z[25|wWijk|i[6]j[6]k[6]] ∈ G[12W]^2)
- s[25]={s[25|wWijk|i[6]j[6]k[6]]}∈A[125]
- Y[2]=(P[2],r[2])∈G[12W],
- Z[25]={Y[2]}[|wWijk|i[6]j[6]k[6]]
- M[2]={M[2|wWijk|]}[|wWijk|] (M[2|wWijk|] ∈ G[12W])
- x[2]=(P[2],Q[2])=({P[2|wWijk|]},{Q[2]
  [|wWijk|]})
  (P[2|wWijk|], Q[2|wWijk|]∈G[12W]),
- r[2]={r[2|wWijk|]}, r[2|wWijk|]∈{}W[12]

暗号方式 E[2]、E[25]をそれぞれ、真理値群環上の多重配列エルガマル暗号、真理値群環上の拡張多重配列エルガマル暗号と呼ぶ事にする。[その他の記号]

- h[:||w|](ijk))=(i□[|w|]j)○k
- F[25:||λ[|1|], λ[|2|], λ[|2|]|](x[2])=
  {x[2:||wh[|w|](ijk)|]
  δ(i,i[6]○λ[|1w|]),
  δ(j,j[6]○λ[|2w|]),
  δ(k,k[6]○λ[|3w|])}
  (wWii[6]jj[6]kk[6]に関する属)。
- J[2](x[2]) ∈ A[12]=J[2](x[2])={x[2|W(w)i[W]|]、
- π[2](a[25])={Σa[25|wWijk|i[6]j[6]k[6]]}[|ijk|]}
  (和はi[6]、j[6]、k[6]に関する和)

ただしここで

- $\lambda[|1|]=\{\lambda[|1w|]\}$、$\lambda[|2|]=\{\lambda[|2w|]\}$、
$\lambda[|3|]=\{\lambda[|3w|]\}$：ビットの属。($w\in C[1]$に関する属)。
- $x[2]=\{x[2|wWh|]\}$ $x[2|wWh|]\in W[12]$,
- 「○」：ビット毎の排他的論理和。
- 「$\square[|w|]$」：素子wで計算する演算子。
(ただしwが入力素子の時は$i\square[|w|]j=1$(if b_wをU_1, …,
U_{l-1}のいずれかが持っている)、$i\square[|w|]j=0$ (othewise)。)
- $\delta(i,i[6])$：クロネッカーのデルタ。
- $i[W]=i$ (if w=L), $i[W]=j$ (if w=R),
- $a[25]=\{a[25|wWijk|i[6]j[6]k[6]]\}\in A[125]$

と定義する。簡単な計算から、次が成立する事が分かる：

- $(a[25]*b[25])c[25]=a[25]*(b[25]*c[25])$,
- $(a[25]*b[25])P[2]=a[25]*(b[25]\{\}P[2])$,
- $F[25:1|\lambda[3|1|],\lambda[3|2|],\lambda[3|3|]|](1)$
$*F[25:1|\lambda[|1|],\lambda[|2|],\lambda[|3|]|](x[2])$
=
$F[25:1|\lambda[3|1|]\bigcirc\lambda[|1|],\lambda[3|2|]\bigcirc\lambda[|2|],\lambda[3|3|]\bigcirc\lambda[|3|]|](x[2])$
- $F[25:1|\lambda[|1|],\lambda[|2|],\lambda[|3|]|](x[2])$
$*F[25:1|0,0,0|](x[23])=F[25|\lambda[|1|],\lambda[|2|],\lambda[|3|]|](x[2]\bigcirc x[23])$
ただしここで
  - $a[25],b[25],c[25]\in A[125]$,
  - $a[2],b[2]\in A[12]$,
  - $x[2],x[23]\in\kappa$,
  - $\lambda[|1|]=\{\lambda[|1w|]\}$, $\lambda[|2|]=\{\lambda[|2w|]\}$
$\lambda[|3|]=\{\lambda[|3w|]\}$,
$\lambda[3|1|]=\{\lambda[|1w|]\}$、
$\lambda[3|2|]=\{\lambda[|2w|]\}$、
$\lambda[3|3|]=\{\lambda[|3w|]\}$：ビットの配列
  - $l\in\{1,\cdots,N\}$

[第0周目の計算の詳細]

第0周目の計算の詳細を述べる。

U1がBODY10を計算する方法を説明する。

U1は以下を計算する。

- x[:0|wWh|]=0,
- x[2:0|wWh|]
  =
  ϕ[2](x[:0|wWh|]),
- x[:0]
  =
  {x[:0|wWh|]},
- x[2:0]
  =
  {x[2:0|wWh|]},
- λ[:0]={λ[:0|w|]={0},
  λ[L:0]={λ[:0|L(w)|]={0},
  λ[R:0]={λ[:0|R(w)|]={0},
- r[2:0]={r[2:0|wWijk|]}={0} (wWijkに関する属)
- y[:0]=0,
  r[2:0]=y[:0]P[2](=O), Y[2:0]=(P[2],r[2:0])
- s[2:0|S|]={(s[2:0|S|])[|wWijk|i[6]j[6]k[6]]}
  ={0}[|wWijk|i[6]j[6]k[6]],
- s[2:0|T|]={(s[2:0|T|])[|wWijk|i[6]j[6]k[6]]}
  ={0}[|wWijk|i[6]j[6]k[6]],
- s[25U:0]={(s[25U:0|wWijk|i[6]j[6]k[6]]}
  ={0}[|wWijk|i[6]j[6]k[6]],
- (S[2:0],T[2:0],U[25:0]) = (E[2][(Y[2:0]|s[2:0|S|])](r[2:0]P[2])
- E[2][(Y[2:0]|s[2:0|T|])](r[2:0]Q[2:0]),
- E[25][(Y[2:0]|s[25R:0])](F[25:1|λ[L:0], λ[R:0], λ[:0]|](x[2:0])P[2])
- $BODY_1^0$ =
  (Q[2:0],r[2:0]) || (s[2:0],T[2:0],U[25:0]),
  ただしここで
  - w∈{}C[1],W∈ {L,R},h∈{0,1},i,j,k∈{0,1}

[第1周目の計算の詳細]

一周目のマルチパーティ計算を説明する。図15に則して説明する。

[データの取得1501の詳細]

各UIはUI-1からデータDATA1I-1を受け取る。(U1のみは、例外的に自分でデータDATA1I-1=DATA10を計算する)。

[データ中の証明文の検証1502の詳細]

さてUI-1からDATA1I-1 || BODY1I-1 || PROOF1I-1 || SIG1I-1 ||が送られてきたら、UIは$PROOF_1^1$、...,$PROOF_1^{I-1}$の正当性を確認する。この正当性の確認についての詳細は後述する。

[データ中の署名文の検証1503の詳細]

UI は SIG11、…、 SIG1i-1 の正当性を確認する。さらに RAND のハッシュ値 P を計算し、P[2]=(e[|0|]+…+e[|κ-1|])(1+η)P を確認する。

[U1 のみ行う計算 1504 の詳細]

U1 はまず、乱数 RAND を任意に選び、RAND のハッシュ値

$P \in G[1]$

とし、P[2]=(e[|0|]+…+e[|κ-1|])P[2B]とし、BODY1-1= RAND || P[2]とし、そして BODY10 を後で説明する手順に従って自分で作成し、さらに PROOF10=SIG10=ε とし、DATA10=RAND||BODY10||PROOF10||SIG10 とする。

[乱数生成 1505 の詳細]

UI はランダムに以下を選ぶ(ただしかっこ内の記述を満たすように選ぶこと):

- {x[#I|wh|]} (x[#I|w[t]0|]}=0,
  x[0#I|w[t]0|]=1,
  x[#I|wh|]∈K[I], 各x[#I|wh|]の最上位ビットは1)。
- {x[|wWh|]}, x[|wWh|] ∈ {0, 1} (x[#I|wLh|]○x[#I|wRh|]=x[#I|wh|]) {w∈C[1], W∈ {L, R}, h∈ {0, 1}}
- r[2]={r[2|wWijk|]}∈A[12],
- r[2|wWijk|]∈F_p^{κ}⊂B[12]$^{\kappa}$=W[12],
- s[2|S|]={(s[2|S|])[|wWijk|]}∈A[12],
- s[2|T|]={(s[2|T|])[|wWijk|]}∈A[12],
- s[25U]={s[25U|wWijk|i[6]j[6]k[6]]}∈A[125].
- λ[#I]={λ[#I|w|]} (ビットの属, λ[|w[t]|]=0)
- y[#I]∈ F_p⊂ κ

•Wt : 出力素子

入力素子 w に対し、形式的に x[#I|L(w)0|]=x[#I|R(w)1|]=0 と定義する。

以下の記号を定義する。

- x[:I|wWh|]=○x[#γ|wWh|], (γ≦Iの範囲の排他的論理和を取る)。
  x[:I]={x[:I|wWh|]},
  x[2#I|wWh|]=φ[2](x[#I|wWh|]),
  x[2#I]={x[2#I|wWh|]},
  x[2:I|wWh|]=φ[2:I](x[|wWh|]),
  x[2:I]={x[2:I|wWh|]},
- λ[#I]={λ[#I|w|]},
  λ[L#I]={λ[#I|L(w)|]},
  λ[R#I]={λ[#I|R(w)|]},
  λ[:I|w|]=Σλ[#γ|w|], (γ≦Iの範囲の和を取る)
  λ[:I]={λ[:I|w|]},
  λ[L:I]={λ[:I|L(w)|]},
  λ[R:I]={λ[:I|R(w)|]},
- Y[2:I]=(P[2],y[:I]P[2]),
  y[:I]=Σy[#I], (γ≦Iの範囲の和を取る)

提案方式に関し、次の事実が言える。ユーザ達がプロトコルにしたがっている場合、各 UI の送るデータ BODY1I は以下を満たす。

- BODY1I = (Q[2:I],r[2:I]) || (s[2:I],T[2:I],U[25:I])、
- (Q[2:I],r[2:I])=J[2](x[2:I])P[2],y[:I]P[2])、
- (s[2:I],T[2:I],U[25:I])=(E[2][(Y[2:I]|s[2][S:I])](r[2:I]P[2]),
E[2][(Y[2:I]|s[2:I|T|])](r[2:I]Q[2:I]),
E[25][(Y[2:I]|s[25U:I])](F[25:I|λ[L:I],λ[R:I],λ[:I]|](x[2:I])P[2])

ただしここで

- s[2:I|S|]
  =
  Σs[2#γ|S|] （γ≦Iの範囲の和を取る);
- s[2:I|T|]
  =
  Σs[2#γ|T|],
-
  s[25U:I]= [235U:I]+s[25U#I],
  s[235U:I]
  =
  F[25:I|λ[L#I], λ[R#I], λ[#I]|](1)
  * s[25U:I-1]
  * F[25:I|0,0,0|](x[2#I]),

[本計算 1506 の詳細]

一周目のマルチパーティ計算の本計算 1506 を図１７に則して説明する。

UI が BODY1I を計算する方法を説明する。

[再暗号用の公開鍵の計算 1701]

UI はまず、

- Q[2:I]=J[2]x[2#I])Q[2:I-1]
- r[2:I]=y[#I]P[2]+r[2:I-1]を計算する。

[データの変換 1702]

- S[23:I]=r[2#I]s[2:I-1]
- T[23:I]=r[2#I]J[2](x[2#I])T[2:I-1]
- U[235:I]=F[25:I|λ[L#I],λ[R#I],λ[#I]|](1)*U[25:I-1]*F[25:I|0,0,0|](x[2#I])

を計算する。

なお、この時次が言える：

- Q[2:I]=J[2](x[2:I])P[2]、
- r[2:I]=y[:I]P[2]、
- S[23:I]=E[2][(Y[2:I-1]|s[2:I-1|S|])](r[2:I]P[2]),
- T[23:I]= E[2][(Y[2:I-1]|s[2:I-1|T|])](r[2:I]Q[2:I]),
- U[235:I]=E[25][(Y[2:I-1]|s[235U:I])](F[25:I|λ[L:I],λ[R:I],λ[:I]|](x[2:I])P[2])。

ただしここで

●s[235U:l]=F[25:l|λ[L#l],λ[R#l],λ[#l]|](1)

*s[25U:l-1]*F[25:l|0,0,0|](x[2#l])

[再暗号化-秘密鍵の変換 1703、再暗号化-乱数の変換 1704、正当性証明文の作成 1507、署名文の作成 1508、データの送信 1509]

最後に Ul は以下を計算する。(かっこ内は図中の番号)。

●(1703)s[233:l]=S[23:l|1|],S[23:l|2|]+y[#l]s[2:l|1|]),

・

T[233:l]=T[23:l|1|],T[23:l|2|]+y[#l]T[2:l|1|]),

・

T[2335:l]=(U[235:l|1|],U[235:l|2|]+y[#l]U[25:l|1|]),

●(1704)

s[2:l]=s[233:l]+E[2][(Y[2:l]|s[2#1|S|])](O),

T[2:l]=T[233:l]+E[2][(Y[2:l]|s[2#1|T|])](O)

U[235:l]=(U[235:l|1|],U[235:l|2|]),

U[25:l]=T[2335:l]+E[25][(Y[2:l]|s[25U#l])](O),

(s[2:l],T[2:l],U[25:l])

=(E[2][(Y[2:l]|s[2:l|S|])](r[2:l]P[2]),

E[2][(Y[2:l]|s[2:l|T|])](r[2:l]Q[2:l]),

E[25][(Y[2:l]|s[25U:l])]

(F[25:l][(λ[L:l],λ[R:l],λ[:l]|)](x[2:l]P[2]),

●(1507)

●(1508)

・BODY1l=s[2:l]・DATA1l-1 || BODY1l-1 || PROOF1l-1 の署名 SIG1l を作成。

●(1509)DATA1l=DATA1l-1 || BODY1l || PROOF1l || SIG1lDATA1l を Ul+1

ただしここで

● S[23:l]=E[2][(Y[2:l-1]|s[2:l-1|S|])](r[2:l]P[2]),

● T[23:l]=E[2][(Y[2:l-1]|s[2:l-1|T|])](r[2:l]P[2]),

● U[235:l]=E[25][(Y[2:l-1]|s[25U:l-1])](r[25:l]P[2]),

- S[23:l]=(S[23:l|1|],S[23:l|2|]),
- T[23:l]=(T[23:l|1|],T[23:l|2|]),
- T[23:l]=(T[23:l|1|],T[23:l|2|]),

正当性証明文の作成 1507 の詳細は長いので説明を後にまわす。

DATA1l=(Q[2:l],r[2:l]) || (s[2:l],T[2:l],U[25:l])を Ul+1 に送る。

なお、この時次が言える：

- S[233:l] =E[2][(Y[2:l]|s[2:l-1|S|])](r[2:l]P[2])、
- s[2:l] = E[2][(Y[2:l]|s[2:l|S|])](r[2:l]P[2])。[第 2 周目の計算の詳細]

第二周目の計算の詳細を図 15 に則して説明する。

[データの取得 1501 の詳細]

各 Ul は Ul-1 からデータ DATA2l-1=DATA2l-2 || BODY2l-1 || PROOF2l-1 || SIG2l-1 を受け取る。

[データ中の証明文の検証 1502、データ中の署名文の検証 1503、U1 のみ行う計算 1504、乱数生成 1505 の詳細、Fp 上の暗号の算出 1801]

以下の計算を行う。

- (1502)PROOF21 || ... || PROOF2l-1 の正当性検証(詳細は後述)。
- (1503)SIG21 || ... || SIG2l-1 の正当性検証
- (1504)何もしない
- (1505)何もしない

[本計算 1506 の詳細]

第二周目の計算の本計算 1506 の詳細を図 18 に則して説明する。

[Fp 上の暗号の算出 1801]

この節では以後添字「:N」を省略する。

Ul は以下の計算をする：

- s[2U]=π[2](s[25U]),
- m[2S]= r[2],
- m[2T]= r[2]J[2](x[2]),
- m[2U]= F[25|λ[L],λ[R],λ|](x[2]),
- U[2]=π[2](U[25])

●(s[2],T[2],U[2])

=E[2][(Y[2]|s[2|S|])](m[2S]P[2]),

E[2][(Y[2]|s[2|T|])](m[2T]P[2]),

E[2][(Y[2]|s[2U])](m[2U]P[2])

ただしここで

●X={(P,x[|wh|]P)}、Y={(P,yP)},

●E[1][(r|X)](A)={E[7][(r[|wWijk|]|X)](A[|wWijk|]P)}

●E[7]：楕円 ElGamal 暗号方式の暗号化関数。

さらに以下の計算をする。

- (s[24V|wWijk|]=Σs[2V|αwWijk|],(αに関する和を取る)
- (m[24V|wWijk|]=Σ2αm[2V])[|αwWijk|],(αに関する和を取る)
- (s[24V|wWijk|]P[2B||]=Σ2αs[2V|αwWijk|]P[2]),(αに関する和を取る)
- s[24V]P[2B]=(s[4V|0,wWijk|]P,s[4V|1,wWijk|]P),
- (m[24V|wWijk|]+(s[24V|wWijk|]y)P[2B]
  =
  Σ2αm[2V|αwWijk|]+s[2V|αwWijk|])yP[2B](αに関する和を取る)
-
-

・ ただしここで

- (s[2V|wWijk|]
  =
  Σs[2V|αwWijk|]e[α] (αに関する和を取る)
- (s[24V|wWijk|]=((s[V|0,wWijk|],(s[V])[|1,wWijk|])
- (m[2V|wWijk|]=m[2V|wWijk|]
  =
  Σm[2Vα|wWijk|]e[|α|],(αに関する和を取る)
- m[24V|wWijk|]=(m[4V|0,wWijk|],m[4V|1,wWijk|]),
- P[2]
  =
  Σe[|α|]P[2B] (αに関する和を取る)
- P[2B]=(P,P), P∈{|G[1],
- V[2]
  =
  E[2][(Y[2]|s[2V])](r[2]P[2])
  =
  (s[2V]P[2],m[2V]P[2]+s[2V]r[2]),
- s[2V|wWijk|]P[2]
  =
  Σ(s[2Vα|wWijk|]e[|α|]P[2B], (αに関する和を取る)
- (m[2V|wWijk|]+s[2V|wWijk|]・y)P[2B] ∈ W[12]
  =
  Σ(((m[2V])[|α|])[|wWijk|]+s[2V|α||wWijk|]yP[2B]e[|α|]。
  (αに関する和を取る)
- (m[24V|wWijk|]+s[24V|wWijk|]y)P[2B]
  =
  (m[4V|0,wWijk|]+s[V|0,wWijk|]y)P,
  (m[4V|1,wWijk|]+s[V|0,wWijk|]y)P

よってUIは以下を得る事ができる：

- s[V|0,wWijk|]P、s[V|1,wWijk|]P,
- m[4V|0,wWijk|]+s[V|0,wWijk|]y)P,

m[4V|1,wWijk|]+s[V|0,wWijk|]y)P,

さらに以下を計算する。

●R=yP、Y=(P,R)

●(s[V|0,wWijk|]P,

(m[4V|0,wWijk|]+s[V|0,wWijk|]y)P

=E[(s[V|0,wWijk|]|Y)](m[4V|0,wWijk|]P),

●(S,T+U)

=(E[3][(s[4S0],s[4T0]+s[4U0]|Y)],E[1][(r[40]|J(X))](F[|λ[L],λ[R],λ|](x))

●{(Θ[|wWijk|],Θ'[|wWijk|])}

=E[3][(s[4S0],s[4T0]+s[4U0]|Y)],E[1][(r[40]|J(X))](F[|λ[L],λ[R],λ|](x))

●Θ[&0]={(Θ[|wWij0|],Θ'[|wWij0|])}

●R[&0]=R0

ただしここで

●r[2]=R[|0|]+R[|1|]η

[Θ[&1]の計算 1802,正当性証明文の作成 1507 の詳細,署名文の作成 1508 の詳細,データの送信 1509 の詳細]

さらに以下の計算を行う：

●(1802)

●Θ[&1]=Θ[&I-1]-(Θ[|0|][&I-1],Θ[|1|][&I-1]-y[&I]Θ[|0|][&I-1]),

●BODY2I=Θ[&I]。

ただしここで

●BODY2I-1=Θ[&I-1],

●Θ[&I-1]=(Θ[&I-1][0],Θ[&I-1|1|])

●(1508)

●(1803)

●BODY2I = s[2:I]

●SIG2I：DATA2I-1 || BODY2I || PROOF2I への署名

そして DATA2I=DATA2I-1 || BODY2I || PROOF2I || SIG2I を UI+1 に送信する(1509)。

[第３周目の計算の詳細]

３周目の計算の詳細を図１５に則して説明する。

U_{l-1} から $DATA_3^{l-1}$=DATA3l-2 || BODY3l || PROOF3l || SIG3l が送られてきたら(1501)、まず $PROOF_3^1$、…、PROOF3l-1、SIG3l、…、SIG3l-1 の正当性を確認する(1502,1503)。(1504),(1505)は第三周目の計算ではない。BODY3l=ε とし(1506)、PROOF3l=ε とし(1507)、そして DATA3l-1 || BODY3l || PROOF3l に対する署名 SIG3l を作成し(1508)、DATA3l=DATA3l-1 || BODY3l || PROOF3l || SIG3l とし、DATA3l を Ul に送る(1509)。

[C[1]({b[|w|]})を求める方法 1405]

C[1]({b[|w|]})を求める方法を説明する。

まず入力素子 w に対して x[#l|L(w)0|]=x[#l|R(w)1|]=0 であるので、{E[1][(|{X[|W(w)i[|W|]|]})]x[|wWh[3](ij0)|]}を全て解き、Xx[|wWh[3](ij0)|]=x[|wWμ[w]|]を求め、x[3|w|]=x[|wμ[w]|]=x[|wLμ[w]|]○{}x[|wRμ[w]|]を計算し、μ[w]=h[3](ij0)とする。

さて、下から u-1 段目までの各素子 w に対して、x[|μ[|w|]|]が求まっているとする。

以下の計算をして u 段目の x[|μ[|w|]|]を求める。

●E[1][(|X[|L(w)μ[|L(w)|]|])]
(x[|{wWh[3](μ[|L(w)|]j0)}|]),
E[1][(|X[|R(w)μ[|R(w)|]|])]
(x[|wWh[3](iμ[|R(w)0)|]|])　(i,j=0,1)
を x[|W(w)μ[|W(w)|]|]を使って解く。

●x[|wh[3]μ[|L(w)|]μ[|R(w)0|]|]=
○x[|wWh[3]μL(w)μ[|R(w)0|]|]
(W に関する排他的論理和)

ただしここで

●h[3](ijk)=h[|w|]((i○λ[|L(w)|])(j○λ[|R(w)|])(k○λ[|w|]))

●μ[w]=b[|w|]○λ[|w|]とし、

●b[|w|]：素子 w の出力

●x[3|w|]=x[|wμ[w]|]

最終的に x[|μ[|w[|t|]|]|]=μ[|[|w[|t|]|]|]=b[|[|w[|t|]|]|]=C[1]({b[|w|]})を出力。

[一周目の計算の正当性証明]

[一周目の計算の正当性証明の作成 1507 の詳細]

以下の記号を定義する：

- A[12|F_p|]={{a[2|wWijk|]}|a[2|wWijk|]∈F_p}、
- F[25:||a[|0|]b[|0|]c[|0|]|a[|1|]b[|1|]c[|1|]](u[2])∈A[12]を
  F[25:||abc|a[|6|]b[|6|]c[|6|]](u[2])
  =
  {x[2|h[:||wa[|iOi[6]|]b[|jOj[6]|]c[|kOk[6]|]|]|](ijk)}
- ただしここで
  - w：素子
  - z[2]∈K[12],
  - a[2]∈A[12],
  - a[25]∈A[125],
  - a[|0|],a[|1|],b[|0|],b[|1|],c[|0|],c[|1|],∈ F_p,
  - u[2]∈K[12],

この節では、簡単の為添字「:l-1」を省略する。

以下の方法で知識を証明する。

まず乱数をハッシュ関数にいれて

P[6]∈G[1]

を作る。そして以下を計算する。

•P[26B]=(1+η)P,

•P[26]=ΣP[26B]e[|α|]、(αに関する和を取る)

•NOT(λ)={NOT(λ[|w|])}

UI は以下の手順で PROOF1I を作成する。ランダムかつ一様に以下のデータを選ぶ。

x[26#I]∈α,

ρ[26#I|S[23]|]∈A[12]2,

ρ[26#I|S[233]||2|]∈A[12],

ρ[26T[2&1]#I]∈A[12]2,

ρ[26T[233]#I]∈A[12]2,

ρ[26T[233]#I|2|]∈A[12],

ρ[246#I|T[233]||2|]∈A[12]2,

ρ[256#I|U[25&1]|]∈A[125]2,

ρ[256#I|λ|]∈A[125],

ρ[256#I|U[25&2]|]∈A[125],

ρ[256#I|U[25&3]|]∈A[125],

ρ[256#I|U[235:I]|]∈A[125]

ρ[256#I|T[2335:I]||2|]∈A[12].

そして以下を計算する。

●C[2x[2]#I|[|αwWh|]|]=x[2#I|αwWh|]P[2B]+(x[26#I|αwWh|]P[26B],C[2x[2]#I]={Σe[|α|]C[2x[2]#I|[|αwWh|]|]}[|wWh|]、(αに関する和を取る)

●C[2#I|S[23]|] = S[23:I] +ρ[26S[23]#I]P[26],τ[S[23]#I]=ρ[26S[23]#I],

●C[2S[23]#I]=(C[2S[23]#1|1|],(C[2S[23]#1])[|2|]) を (C[2S[23]#I|1|],C[2S[23]#I|2|]) と書く。

C[y,C[2S[23]]#I|1|]

=

yC[2S[23]#I|1|] +ρ[26S[233]#I|2|]P[26||]{A[12]},

C[2S[233]#I]=(C[2S[23]#I|1|],C[2S[233]#I|2|]),

C[2S[233]#I|2|]=C[2S[23]#I|2|]+C[2y,C[2S[23]]#I|1|],

τ[S[233]#I]=(τ[S[23]#I|1|],

τ[S[23]#I|2|]+yτ[S[23]#I|1|]+ρ[26S[233]#I])。

ただしここで(τ[S[23]#I|1|]、τ[S[23]#I|2|]) =(τ[S[23]#I])。

●C[2T[2&1]#I]=T[2&1:I]+ρ[26T[2&1]#I]P[26]を,τ[T[2&1]#I] = ρ[26T[2&1]#I],

●C[2T[233]#I]=T[233:I] +ρ[26T[233]#I]P[26],τ[T[233]#I]=ρ[26T[233]#I],

●C[2T[23:I]#I]=(C[2T[23:I]#I|1|],C[2T[23:I]#I|2|])を(C[2T[23:I]#I|1|],C[2T[23:I]#I|2|])と書く。

C[y,C[2T[23:I]]#I|1|]=yC[2T[23:I]#I|1|] +ρ[26T[233]#I|2|]P[26A[12]],

C[2T[233]#I]=(C[2T[23:I]#I|1|],C[2T[233]#I|2|]),

C[2T[233]#I|2|]=C[2T[23:I]#I|2|]+C[2y,C[2T[23:I]]#I|1|],

τ[T[233]#I]=(τ[T[23:I]#I|1|],

τ[T[23:I]#I|2|]+yτ[T[23:I]#I|1|]+ρ[26T[233]#I])。

ただしここで(τ[T[23:I]#I|1|]、τ[T[23:I]#I|2|]) =τ[T[23:I]#I]。

●K[2y,C[2T[233]]#I|1|]=y[4#I]C[2T[23:I]]+ρ[246T[233]#I|1|]P[26],

●c[25U[25&1]#I]=U[25&1:I]+ρ[256#I|U[25&1]]]P[26],τ[U[25&1]#I]=ρ[256#I|U[25&1]]]。

●C[2λ#I]=λ[#I]P[2]+ρ[256#I|λ|]P,

●ρ[256NOT(λ)#I]=-ρ[256λ#I],C[2NOT(λ)#I]=P[2]-C[2λ#I],

●C[2U[25&2]#I]=F[25:I|λ[L]{}00|NOT(λ)[L]00](u[2])C[2U[25&1]#I]+ρ[256#I|U[25&2]|]P[26],

ただしここで NOT(λ)[L]={NOT(λ)[|L(w)|]}。

τ[U[25&2]#I]=F[25:I|λ[L]{}00|NOT(λ)[L]00](u[2])τ[U[25&1]#I]+ρ[256#I|U[25&2]|],

●C[2U[25&3]#I]=F[25:I|0λ[R]0|0NOT(λ)[R]0](u[2])C[2U[25&2]#I]+ρ[256U[25&3]#I]P[26],

ただしここで

NOT(λ)[R]={NOT(λ)[R|R(w)|]}。

τ[U[25&3]#I]=F[25:I|0λ[R]0|0NOT(λ)[R]0](u[2])τ[U[25&2]#I]+ρ[256U[25&3]#I]。

●C[2U[235:I]#I]=F[25:I|00λ|00NOT(λ)](u[2])C[2U[25&3]#I],

τ[U[235:I]#I]=F[25:I|00λ|00NOT(λ)](u[2])τ[U[25&3]#I],

●C[2U[235:I]#I]=((C[2U[235:I]#I])[|1|],(C[2U[235:I]#I])[|2|])を

(C[2U[235:I]#I|1|],C[2U[235:I]#I|2|])と書く。

C[y,C[2U[235:I]]#I|1|]=yC[2U[235:I]#I|1|] +ρ[256#I|T[2335:I]||2|]P[26A[12]],

C[2T[2335:I]#I]=(C[2U[235:I]#I|1|],C[2T[2335:I]#I|2|]),

C[2T[2335:I]#I|2|]=C[2U[235:I]#I|2|] +C[2y,C[2U[235:I]]#I|1|],

τ[T[2335:I]#I]=(τ[U[235:I]#I|1|],

τ[U[235:I]#I|2|]+yτ[U[235:I]#I|1|]+ρ[256T[2335:I]#I]),

ただしここで(τ[U[235:I]#I|1|]、τ[U[235:I]#I|2|]) =τ[U[235:I]#I]。

さらに以下の計算をする。

● x[2|αwWh|]P[2B]=1の時。

- 各αwWhに対し、
  まずランダムにx[246&1|αwWh|]∈B[1]を選び、K[2&1|αwWh|]=
  x[246&1|αwWh|]P[26B]
  を計算。
- ランダムに
  x[29&η|αwWh|],
  c[2&η|αwWh|]∈B[1]を選び、
  K[2&η|αwWh|]
  =
  x[29&η|αwWh|]P[26]
  −c[2&η|αwWh|](C[2x[2]|αwWh|]−ηP[2B])を計算する。

●x[2|αwWh|]P[2B]=η の時。

- 各αwWhに対し、
  まずランダムにx[246&η|αwWh|]∈B[1]を選び、K[2&η|αwWh|]=
  x[246&η|αwWh|]P[26B]を計算する。
- ランダムに
  x[29&1|αwWh|]，c[2&1|αwWh|]
  ∈B[1]を選び、
  K[2&1|αwWh|]=x[29&1|αwWh|]P[26]
  -c[2&1|αwWh|](C[2x[2]|αwWh|]-P[2B])を計算し、
  (K[2&1|αwWh|],
  (K[2&η|αwWh|]を計算する。

さらに以下のデータを一様かつランダムに選ぶ。

x[24#I], x[246#I] ∈ A[12],

y[4#I]∈ F_p,

r[24#I]∈A[12F_p]、
ρ[246S[23]#I]∈A[12]^2,

ρ[246S[233]#I|2|]∈A[12]^2,

s[24S#I]∈A[125]、 τ[4S[233]#I]∈A[125]^2,

r[24#I]∈A[12F_p]、
ρ[246T[2&1]#I]∈A[12]^2,

ρ[246T[233]#I]∈A[12]^2,

s[24T#I]∈A[125]、 τ[4T[233]#I]∈A[125]^2,

ρ[2456U[25&1]#I]
∈ A[125]^2,

ρ[2456 λ#I]∈A[125],
λ[4#I]∈F_p,

NOT(λ)[4#I],
=
{NOT(λ)[4#I|w|]},
NOT(λ)[#I|w|]
∈ F_p,
ρ[2456U[25&2]#I]∈ A[125],

ρ[2456T[2335:I]#I|2|]∈A[12]^2,

s[245U#I]∈A[125]、 τ[4T[2335:I]#I]∈A[125]^2,

そして以下を計算する。

●K[2x[2]#I]=x[24#I]P[2]+x[246#I]P[26],

●K[2J[2](x),Q[2]#I]=J[2](x[24])Q[2],

K[2y#I]a=y[4#I]P∈ F_p⊂ B[1],

●K[2r[2],s[2]#I]=r[24#I]s[2]+ρ[246S[23]#I]P[26],

●K[2y,C[2S[233]]#I|1|]=y[4#I]C[2S[23]]+ρ[246S[233]#I|1|]P[26],

●K[2s[24S]#I]=s[24S#I]Y[2]-τ[4S[233]#I]P[26],

●K[2r[2],T[2]#I]=r[24#I]T[2]+ρ[246T[2&1]#I]P[26],

●K[2J[2](x[2]),T[2&1]#I]=J[2](x[24#I])T[2&1]+ρ[246T[233]#I]P[26],

●K[2s[24T]#I]=s[24T#I]Y[2]-τ[4T[233]#I]P[26],

●K[25U[25&1]#I] =U[25:I-1]*F[25:I|0,0,0|](x[24#I])+ρ[2456U[25&1]#I]P[26],

●K[2λ,P[2]#I]=λ[4#I]P[2]+ρ[2456λ#I]P[26],K[2λ,C[2λ]#I]=λ[4#I]C[2λ#I]+ρ[2456λ#I]P[26],

●λ[4L#I]={λ[4#I|L(w)|]},NOT(λ)[4L#I]={NOT(λ)[4#I|L(w)|]},K[2U[25&2]#I]=F[25:I|λ[4L]00|NOT(λ)[4L]00](1)*U[25&1]+ρ[2456U[25&2]#I]P[26],

●λ[4R#I]={λ[4#I|R(w)|]},NOT(λ)[4R#I]={NOT(λ)[4R(w)#I]},K[2U[25&3]#I]=F[25:I|0λ[4R]0|0NOT(λ)[4R]0](1)*U[25&2]+ρ[2456U[25&3]#I]P[26],

●λ[4R#I]={λ[4R(w)#I]},NOT(λ)[4R#I]={NOT(λ)[4R(w)#I]},K[2U[235:I]#I]=F[25:I|00λ[4]|00NOT(λ)[4]](1)*U[25&3],

●K[2y,C[2T[2335:I]]#I|1|]=y[4#I]C[2U[235:I]]+ρ[2456T[2335:I]#I|1|]P[26],

●K[2s[245U]#I]=s[245U#I]Y[2]-τ[4T[2335:I]#I]P[26],

さらに以下を計算する。

さらに

c[#I]=Hash(DATA1I-1,BODY1I,C[2x[2]#I],C[2S[23]#I],(C[2S[23]#I|1|],C[2S[23]#I|2|]),C[y,C[2S[23]]#I|1|],C[2T[2&1]#I],C[2T[233]#I],(C[2T[23:I]#I|1|],C[2T[23:I]#I|2|]),C[2T[233]#I],K[2s[24T]#I]=s[24T#I]Y[2]c[25U[25&1]#I],C[2λ#I],C[2NOT(λ)#I],C[2U[25&2]#I],C[2U[25&3]#I],C[2U[235:I]#I],(C[2U[235:I]#I|1|],C[2U[235:I]#I|2|]),C[y,C[2U[235:I]#I|1|],C[2T[2335:I]#I|2|],K[2&1|αwWh|],K[2&η|αwWh|],K[2x[2]#I],K[2J[2](x),Q[2]#I],K[2y#I],K[2r[2],s[2]#I],K[2y,C[2S[233]]#I|1|],K[2s[24S]#I],K[2r[2],T[2]#I],K[2J[2](x[2]),T[2&1]#I],K[25U[25&1]#I],K[2λ,P[2]#I],K[2λ,C[2λ]#I],K[2U[25&2]#I],K[2U[25&3]#I],K[2U[235:I]#I],K[2y,C[2T[2335:I]]#I|1|],K[2s[245U]#I],)を計算する。

ただしここでHashは、Fp値ハッシュ関数。

そして次を計算。

●x[2|αwWh|]P[2B]=1の時。

●各αwWhに対し、c[2&1|αwWh|]=c[#l]-c[2&η|αwWh|]とし、

x[29&1|αwWh|]=c[2&1|αwWh|](x[26|α|])[|wWh|]+x[246&1|αwWh|]を計算。

●x[2|αwWh|]P[2B]=ηの時。

●各αwWhに対し、c[2&η|αwWh|]=c[#l]-c[2&1|αwWh|]とし、

x[29&η|αwWh|]=c[2&η|αwWh|](x[26|α|])[|wWh|]+x[246&η|αwWh|]を計算

(c[#l]c[2&1|αwWh|],x[29&1|αwWh|]),c[2&η|αwWh|] ,x[29&η|αwWh|]))する。

さらに次を計算。

●x[28#l]=c[#l]x[2#l]+x[24#l] ,x[268#l]=c[#l]x[26#l]+x[246#l],

●y[8#l]=c[#l]y[#l]+y[4#l],

●r[28#l]=c[#l]r[2#l]+r[24#l],ρ[268S[23]#l]=c[#l]ρ[26S[23]#l]+ρ[246S[23]#l],

●r[8#l]=c[#l]r[2#l]+r[24#l],ρ[268S[233]#l|2|]=c[#l]ρ[26#l|S[233]||2|]+ρ[246S[233]#l|2|

],

●s[28S#l]=c[#l]s[24S#l]+s[24S#l]、τ[8S[233]#l]=c[#l]τ[S[233]#l]+τ[4S[233]#l],

●r[28#l]=c[#l]r[2#l]+r[24#l],ρ[268T[2&1]#l]=c[#l]ρ[26T[2&1]#l]+ρ[246T[2&1]#l],

●ρ[268T[233]#l]=c[#l]ρ[26T[233]#l]+ρ[246T[233]#l],

●r[8#l]=c[#l]r[2#l]+r[24#l],ρ[268T[233]#l|2|]=c[#l]ρ[26T[233]#l|2|]+ρ[246#l|T[233]||2|]

,

●s[28T#l]=c[#l]s[24T#l]+s[24T#l]、τ[8T[233]#l]=c[#l]τ[T[233]#l]+τ[4T[233]#l],

●ρ[2568U[25&1]#l]=c[#l]ρ[256U[25&1]#l]+ρ[2456U[25&1]#l],

●λ[8#l]=c[#l]λ[#l]+λ[4#l],ρ[2568λ#l]=c[#l]ρ[256λ#l]+ρ[2456λ#l],

●NOT(λ)[8#l]=c[#l]NOT(λ)[#l]+NOT(λ)[4#l]

ρ[2568U[25&2]#l]=c[#l]ρ[256U[25&2]#l]+ρ[2456U[25&2]#l]P[26],

●ρ[2568U[25&3]#l]=c[#l]ρ[256U[25&3]#l]+ρ[2456U[25&3]#l]P[26],

●r[8#l]=c[#l]r[2#l]+r[24#l],ρ[2568T[2335:l]#l|2|]=c[#l]ρ[256T[2335:l]#l|2|]+ρ[2456T[2

335:l]#l|2|],

●s[258U#l]=c[#l]s[245U#l]+s[245U#l]

τ[8T[2335:l]#l]=c[#l]τ[T[2335:l]#l]+τ[4T[2335:l]#l]。

そして、

PROOF1l=(C[2x[2]#l],C[2S[23]#l],(C[2S[23]#l|1|],C[2S[23]#l|2|]),C[y,C[2S[23]]#l|1|],C[2T[2&1]#l],C[2T[233]#l],(C[2T[23:l]#l|1|],C[2T[23:l]#l|2|]),C[2T[233]#l],c[25U[25&1]#l],C[2λ#l],C[2NOT(λ)#l],C[2U[25&2]#l],C[2U[25&3]#l],C[2U[235:l]#l],(C[2U[235:l]#l|1|],C[2U[235:l]#l|2|]),C[y,C[2U[235:l]]#l|1|],C[2T[2335:l]#l|2|],K[2&1|αwWh|],K[2&η|αwWh|],K[2x[2]#l],K[2J[2](x),Q[2]#l],K[2y#l],K[2r[2],s[2]#l],K[2y,C[2S[233]]#l|1|],K[2s[24S]#l],K[2r[2],T[2]#l],K[2J[2](x[2]),T[2&1]#l],K[2s[24T]#l],K[25U[25&1]#l],K[2λ,P[2]#l],K[2λ,C[2λ]#l],K[2U[25&2]#l],K[2U[25&3]#l],K[2U[235:l]#l],K[2y,C[2T[2335:l]]#l|1|],K[2s[245U]#l],c[#l],x[29&1|αwWh|]),x[29&η|αwWh|])),x[28#l] ,x[268#l],y[8#l],r[28#l],ρ[268S[23]#l]r[8#l]ρ[268S[233]#l|2|]s[28S#l]r[28#l]ρ[268T[2&1]#l]ρ[268T[233]#l]r[8#l]ρ[268T[233]#l|2|]ρ[2568U[25&1]#l],λ[8#l] ,ρ[2568λ#l] ,NOT(λ)[8#l],ρ[2568U[25&2]#l],ρ[2568U[25&3]#l],r[8#l]ρ[2568T[2335:l]#l|2|]s[258U#l])とする。

[一周目の計算の正当性証明の検証 1502 の詳細]

PROOF1l を受け取ったら、Ul+1 は以下を確認する。

•

c[#l]=Hash(DATA1l-1,BODY1l,C[2x[2]#l],C[2S[23]#l],(C[2S[23]#l|1|],C[2S[23]#l|2|]),C[y,C[2S[23]]#l|1|],C[2T[2&1]#l],C[2T[233]#l],(C[2T[23:l]#l|1|],C[2T[23:l]#l|2|]),C[2T[233]#l],K[2s[24T]#l]c[25U[25&1]#l],C[2λ#l],C[2NOT(λ)#l],C[2U[25&2]#l],C[2U[25&3]#l],C[2U[235:l]#l],(C[2U[235:l]#l|1|],C[2U[235:l]#l|2|]),C[y,C[2U[235:l]]#l|1|],C[2T[2335:l]#l|2|],K[2&1|αwWh|],K[2&η|αwWh|],K[2x[2]#l],K[2J[2](x),Q[2]#l],K[2y#l],K[2r[2],s[2]#l],K[2y,C[2S[233]]#l|1|],K[2s[24S]#l],K[2r[2],T[2]#l],K[2J[2](x[2]),T[2&1]#l],K[25U[25&1]#l],K[2λ,P[2]#l],K[2λ,C[2λ]#l],K[2U[25&2]#l],K[2U[25&3]#l],K[2U[235:l]#l],K[2y,C[2T[2335:l]]#l|1|],K[2s[245U]#l],),

•各 αwWh に対し、以下が成立する事。

•c[#l]=c[2&1|αwWh|]+c[2&η|αwWh|] ,x[29&1|αwWh|] P[6B]=c[2&1|αwWh|](C[2x[2]|αwWh|]-P[2B])+K[2&1|αwWh|],x[29&1|αwWh|] P[6B]=c[2&η|αwWh|](C[2x[2]|αwWh|]-ηP[2B])+K[2&η|αwWh|]

●以下が成立する事

- x[28#I]P[2]+x[28#I]P[26] =
  c[#I]C[2x[2]#I]+K[2x[2]#I],
- J[2](x[28#I])Q[2#I] = J[2](c[#I])Q[2#I]+K[2J[2](x),Q[2]#I],
- y[8#I] ∈ F_p,
  y[8#I]P[2] = c[#I](r[2:I]−r[2]) +K[2y#I],
- y[8#I] ∈ F_p,
- r[28#I]s[2:I−1]
  +
  ρ[268S[23]#I]P[26]
  =
  c[#I]C[2S[23]#1] + K[2r[2],s[2]#I],
- c[#I]C[2y,C[2S[23]]#I|1|]
  +
  K[2y,C[2S[23]]#I|1|]
  =
  y[8#I]C[2S[23]#I|2|]
  +
  ρ[268S[233]#I|2|]P[26A[12]],
- c[#I](s[2#I]−C[2S[233]#I])
  +
  K[2s[24S]#I]
  =
  s[28S#I]Y[:I]
  −
  τ[8S[233]#I]P[2],
- r[28#I]T[2:I−1]
  +
  ρ[268T[2&1]#I]P[26]
  =
  c[#I]C[2T[2&1]#I] + K[2r[2],T[2]#I],
- J[2](x[28#I])T[2&1:I−1]
  +
  ρ[268T[233]#I]P[26]
  =
  c[#I]C[2T[233]#I] + K[2r[2],T[2&1]#I],
- c[#I]C[2y,C[2T[23:I]]#I|1|]
  +
  K[2y,C[2T[23:I]]#I|1|]
  =
  y[8#I]C[2T[23:I]#I|2|]
  +
  ρ[268T[233]#I|2|]P[26A[12]],

を確認する。

- c[#I](T[2#I]-C[2T[233]#I])
  +
  K[2s[24T]#I]
  =
  s[28T#I]Y[:I]
  -
  τ[8T[233]#I]P[2],
- r[28#I]∈A[12F_p],
- U[25:I-1]*F[25:I|0,0,0|](x[28#I])
  +
  ρ[2568U[25&1]#I]P[26]
  =
  c[#I]c[25U[25&1]#I]
  +
  K[25U[25&1]#I],
- 各wWijk,i[6],j[6],k[6]に対し
  λ[8#I|wWijk|i[6],j[6],k[6]]∈ F_pとなる事、

λ[8#I]P[2]+ρ[2568λ#I]P[26]=c[#I]C[2λ#I]+K[2λ,P[2]#I],λ[8#I]C[2λ#I]+ρ[2568λ#I]P[26]=c[#I]C[2λ#I]+K[2λ,C[2λ]#I],

●C[2NOT(λ)#I]=P[2]-C[2λ#I],

●c[#I]C[2U[25&2]#I]+K[2U[25&2]#I]=F[25:I|λ[8L]00|NOT(λ)[8L]00](1)*U[25&1]+ρ[2568U[25&2]#I]P[26],

●c[#I]C[2U[25&3]#I]+K[2U[25&3]#I]=F[25:I|λ[8R]00|NOT(λ)[8R]00](1)*U[25&2]+ρ[2568U[25&3]#I]P[26],

●c[#I]C[2U[235:I]#I]+K[2U[235:I]#I]=F[25:I|{00λ[8]|00NOT(λ)[8]](1)*U[25&3],

●c[#I]C[2y,C[2U[235:I]]#I|1|]+K[2y,C[2U[235:I]]#I|1|]=y[8#I]C[2U[235:I]#I|2|]+ρ[2568T[2335:I]#I|2|]P[26A[12]],

●c[#I](U[2#I]-C[2T[2335:I]#I])+K[2s[245U]#I]=s[258U#I]Y[:I]-τ[8T[2335:I]#I]P[2]。

[二周目の計算の正当性証明]

[二周目の計算の正当性証明の作成 1507 の詳細]

UI はランダムに

$$y[4\&I] \in F_p$$

を選び、以下のようにして PROOF2I を計算する。

- P[4&I]=y[4&I]P,Θ[4&I|1|]=y[4&I]Θ[&I|1|],
- c[&I]=Hash(DATA2I-1 || BODY2I-1|| P[4&I] || Θ[4&I]),
- y[8&I]=c[&I]y[&I]+y[4&I],
- PROOF2I=P[4&I] || Θ[4&I]|| c[&I] || y[8&I]。

[二周目の計算の正当性証明の検証 1502 の詳細]

PROOF1I を受け取ったら、UI+1 は以下を確認する。

- y[8&I]P=c(R[:I]-R[:I-1]})+P[4]
- y[8&I]Θ[8&I-1|0|]=c(Θ[&I-1|0|]-Θ[&I|0|])+Θ[4&I-1|0|]

産業上の利用可能性

電子入札、電子競売等で、落札者以外の入札者の入札値を秘密にしたまま、入札者と入札価格を決定したい場合で、かつその決定が正しく行われたことを第三者が検証できる必要がある場合等や、電子投票等で匿名性を保ったまま正しく票数が数えられていることを第三者が検証できる必要がある場合等に、本発明方法を用いると有効である。

なぜならば、本発明方法を用いれば、上記入札、競売、投票の結果を複数の計算装置で行えば、誰も計算結果以外の情報を新たに得ることがなく、かつその計算の正当性を誰でも検証できるからである。そしてこの計算が従来の技術を持ってして行うより効率的である。さらに、計算装置間の通信回数が少ないため、計算装置が通信に回線を確保するのに時間を費やす時間も少なく、効率的である。

請求の範囲

１．　複数の計算装置を含む機器を用いて与えられた関数の値を計算する方法であって、

入力処理と、

出力処理とからなり、

前記入力処理では、前記複数の計算装置に、回路と、前記回路への入力ビットとが入力され、

まず一台の前記計算装置が計算を行い、その計算結果を他の前記計算装置のうち一台に送り、次にその計算結果を受け取った前記前記計算装置がその次の計算を行う、というとように一台ずつ順に計算を行ってその計算結果を次の一台に回し、全ての前記計算装置が一度ずつ計算が終わったら、最後に計算をした計算装置が最初に計算をした計算装置に計算結果を送り、以後何度も、一台ずつ順に計算を行ってその計算結果を次の一台に回すという各周の計算を繰り返す事を特徴とする計算方法。

２．　複数の計算装置を含む機器を用いて与えられた関数の値を計算する方法であって、

入力処理と、

ElGamal 暗号文準備処理と、

逐次置換再暗号処理と、

結果出力処理とからなり、

前記入力処理は、

前記複数の計算装置に複数のゲートから構成された回路の情報及び前記複数の計算装置に関する情報が入力される、情報入力ステップと、関数の入力データを複数に計算装置の個数に分散したデータである複数の部分データを、それぞれの計算装置にそれぞれ一つずつ入力する分散入力ステップと、からなり、

前記 ElGamal 暗号文準備処理は、少なくとも一つの計算装置が、与えられた関

数を実現する回路のゲートに対応した ElGamal 暗号文の集合を生成する ElGamal 暗号文準備ステップとからなり、

前記逐次置換再暗号処理は、

置換再暗号処理を各計算装置が順番に行う処理で、前記置換再暗号処理は、順番が回ってきた計算装置が、一つ前の順番に対応する計算装置から ElGamal 暗号文の集合を受け取る暗号文取得ステップと、

前記暗号文取得ステップにて受け取った暗号文の集合を順序を入れ替えて置換し、それらを再暗号化する暗号文の置換と再暗号化ステップと、

前記暗号文の置換と再暗号化ステップで生成したデータを、少なくとも次の順番の計算装置に公開するステップと、からなり、

前記結果出力処理は、

前記逐次置換再暗号処理で生成された暗号文の一部を復号あるいは部分復号する部分復号ステップと、

前記前記逐次置換再暗号処理で生成された暗号文の中で前記回路の入力に対応するデータを暗号化している暗号文を復号する復号ステップと、

前記復号ステップで復号されたデータと、前記部分復号ステップで部分復号されたデータを用いて、回路の出力を評価する回路の評価ステップと、からなることを特徴とする計算方法。

3. 複数の計算装置と、

複数の計算装置と通信する手段と、

入力処理手段と、

ElGamal 暗号文準備手段と、

置換再暗号処理手段と、

結果出力処理手段と、からなる関数を評価する計算システムであって、

前記入力処理手段は、出力を求めたい回路の情報と、前記複数の計算装置に関する情報と、前記複数の計算装置がそれぞれ前記回路の入力のどの部分を所持しているかという情報と、を入力し、

前記 ElGamal 暗号文準備処理手段は、与えられた関数を実現する回路のゲート

に対応したElGamal暗号文の集合を生成するElGamal暗号文を準備し、

前記置換再暗号処理手段は、

順番が回ってきた計算装置が、一つ前の順番に対応する計算装置から ElGamal暗号文の集合を受け取る暗号文取得手段と、

前記暗号文取得手段により受け取られた暗号文の集合の順序を入れ替えて置換し、それらを再暗号化する暗号文の置換と再暗号化手段と、

前記暗号文の置換と再暗号化手段を用いて生成したデータを、少なくとも次の順番の計算装置に公開する手段と、からなり、

前記結果出力手段は、

置換再暗号処理手段で生成された暗号文の一部を復号あるいは部分復号する部分復号手段と、

前記前記逐次置換再暗号処理で生成された暗号文の中で前記回路の入力に対応するデータを暗号化している暗号文の自分に関する暗号化を復号する復号手段と、

前記複数の計算機が前記復号手段で復号したデータと前記複数の計算機が前記部分復号手段で部分復号されたデータを用いて回路の出力を評価する回路の評価手段と、からなることを特徴とする計算システム。

4. 請求項2に記載された計算方法において、

前記各ゲートに対応する ElGamal 暗号文の集合は、前記各計算装置が各ゲートに対応して生成した秘密鍵の ElGamal 暗号文の集合であり、

前記 ElGamal 暗号文を生成するのに用いた公開鍵は、このゲートに入力される二つの信号を生成するゲートに対応する公開鍵の和であることを特徴とする計算方法。

5. 前記請求項2に記載された計算方法において、

前記入力処理として、各計算装置に ElGamal 暗号方式の領域変数を入力するステップが行なわれ、

前記 ElGamal 暗号文準備処理として、各前記計算装置が、各前記回路の各ゲートに対応して、ElGamal暗号文の秘密鍵を生成するゲート秘密鍵生成ステップが行

なわれ、

各計算装置では、

前記ゲート秘密鍵の生成ステップにて生成した秘密鍵に対応するゲート公開鍵を生成するゲート公開鍵の生成ステップと、

前記ゲート公開鍵の生成ステップにて生成した公開鍵の正当性の証明を生成するゲート公開鍵の正当性の証明生成ステップと、

前記ゲート公開鍵の正当性の証明生成ステップにて生成したゲート公開鍵の正当性の証明を公開するゲート公開鍵の正当性の証明公開ステップと、

各前記回路のゲートで回路への入力が直接入力されるゲートに対応して、ElGamal 暗号文の秘密鍵を生成する入力のゲート秘密鍵の生成ステップと、

前記入力ゲート秘密鍵の生成ステップにて生成した秘密鍵に対応する入力ゲート公開鍵を生成する入力のゲート公開鍵の生成ステップと、

前記入力のゲート公開鍵の生成ステップにて生成した公開鍵の正当性の証明を生成する入力のゲート公開鍵の正当性の証明生成ステップと、

前記入力のゲート公開鍵の正当性の証明生成ステップにて生成し入力の公開鍵の正当性の証明を公開する入力のゲート公開鍵の正当性の証明公開ステップと、

その他の各計算装置が生成して公開したゲート公開鍵を取得するゲート公開鍵取得ステップと、

前記ゲート公開鍵取得ステップにおいて取得したゲート公開鍵を統合するゲート公開鍵の統合ステップと、

前記ゲート公開鍵の統合ステップにおいて統合したゲート公開鍵により、この計算装置が生成したゲート秘密鍵を暗号化するゲート秘密鍵の暗号化ステップと、

前記ゲート秘密鍵の暗号化ステップにおいて生成したゲート秘密鍵の暗号文を公開するゲート秘密鍵の暗号文の公開ステップと、

前記ゲート秘密鍵の暗号文の正当性証明を生成するゲート秘密鍵の暗号文の正当性の証明生成ステップと、

前記ゲート秘密鍵の暗号文の正当性の証明生成ステップにおいて生成したゲート秘密鍵の暗号文の正当性の証明を公開するゲート秘密鍵の暗号文の正当性の証明公開ステップと、

各計算装置に入力された回路の入力の部分に対応する暗号文を生成する入力の暗号文生成ステップと、

前記入力の暗号文生成ステップにて生成した回路の入力の部分に対応する暗号文の正当性の証明を生成する入力の暗号文の正当性の証明生成ステップと、

前記入力の暗号文の正当性の証明生成ステップにおいて生成した証明を公開する入力の暗号文の正当性の証明公開ステップと、

出力のゲートに対応する暗号文を生成して公開する出力の暗号文の生成ステップと、を含み、

前記置換再暗号処理が、

前記ゲート秘密鍵の暗号文の集合の順番をあらかじめ決められた許された置換の方法から無作為に一つの置換を選んで入れ替えて再暗号化するゲート秘密鍵の暗号文の置換と再暗号化ステップと、

前記入力の暗号文の集合の順番をあらかじめ決められた許された置換の方法から無作為に一つの置換を選んで入れ替えて再暗号化する入力の暗号文の置換と再暗号化ステップと、

前記出力の暗号文の集合の順番をあらかじめ決められた許された置換方法から無作為に一つの置換を選んで入れ替えて再暗号化する出力の暗号文の置換と再暗号化ステップと、

前記ゲート秘密鍵の暗号文の置換と再暗号化ステップと入力の暗号文の置換と再暗号化ステップと出力の暗号文の置換と再暗号化ステップとにおいてなされた置換と再暗号化の正当性の証明を生成し公開するゲート秘密鍵の暗号文と入力の暗号文と出力の暗号文の置換と再暗号化の正当性の証明生成と公開ステップと、を含み、

前記結果出力処理の部分復号ステップが、

前記計算装置が互いに通信及び計算することで前記ゲート秘密鍵の暗号文を部分復号するゲート秘密鍵の部分復号ステップと、

前記計算装置が互いに通信及び計算することで前記入力の暗号文を部分復号する入力の暗号文の部分復号ステップと、

前記計算装置が互いに通信及び計算することで前記出力の暗号文を部分復号す

る出力の暗号文の部分復号ステップと、

前記ゲート秘密鍵の部分復号ステップと入力の暗号文の部分復号ステップと出力の暗号文の部分復号ステップとでなされた部分復号の正当性の証明を生成し公開するゲート秘密鍵と入力の暗号文と出力の暗号文の部分復号ステップの正当性の証明生成と公開ステップと、を含み、

他の計算装置の公開した種々の正当性の証明を検証するステップを含む、ことを特徴とする計算方法。

6. 複数の計算装置、入力手段、出力手段を含み、まず一台の前記計算装置が計算を行い、その計算結果を他の前記計算装置のうち一台に送り、次にその計算結果を受け取った前記前記計算装置がその次の計算を行う、というとように一台ずつ順に計算を行ってその計算結果を次の一台に回し、全ての前記計算装置が一度ずつ計算が終わったら、最後に計算をした計算装置が最初に計算をした計算装置に計算結果を送り、以後何度も、一台ずつ順に計算を行ってその計算結果を次の一台に回すという各周の計算を繰り返す計算システムであって、

前記入力手段では前記計算装置に回路の情報と、前記回路への入力ビットの一部とが入力され、

第ゼロ周目の計算は第一の計算装置が第一周目の計算を行う前に行い、

前記複数の計算装置には、

前記各周の計算に使用される送られてきたデータを取得するデータ取得手段と、正当性証明検証手段と、署名文検証手段と、第一の計算装置のみが行う第一計算装置特別計算手段と、乱数生成を行う乱数生成手段と、本計算を行う本計算計算手段と、本計算で行った計算の正当性を証明する正当性証明作成手段と、署名手段とデータ送信手段とからなり、

前記送られてきたデータは、別の計算装置から送られてきたデータと、データ本体と、データ本体に対する正当性証明と、署名文とからなり、

前記署名文は、前記別の計算装置から送られてきたデータと、前記データ本体と、前記データ本体に対する正当性証明との組に対する署名文であるようなデータで、

前記正当性証明検証手段は前記送られてきたデータ中の正当性証明を検証し、

前記署名検証手段は、前記送られてきたデータ中署名文を検証し、

前記本計算は前記乱数生成手段で生成された乱数を用いて計算し、

前記署名手段が、前記送られてきたデータと、前記本計算で計算された計算結果であるデータ本体と、前記正当性証明作成手段で作成された正当性証明との組に対する署名文を作成し、

前記データ送信手段が、前記送られてきたデータと、前記本計算で計算された計算結果であるデータ本体と、前記正当性証明作成手段で作成された正当性証明と前記署名手段で作成された署名文との組を送信する事を特徴とする計算システム。

7. 請求項6に記載された計算システムにおいて、

前記送られてきたデータのデータ本体と前記本計算で計算されたデータ本体とが、第一周目の計算では、共に真理値群環上の多重配列エルガマル暗号文達と真理値群環上の拡張多重配列エルガマル暗号文達とからなる組である計算システム。

8. 請求項7に記載された計算システムにおいて、

各周の計算が、第一周目の計算手段と、第一周目以降の周の計算手段とからなり、

前記計算手段は、第ゼロ周目の計算手段では真理値群環上の多重配列エルガマル暗号文達と真理値群環上の拡張多重配列エルガマル暗号文達とからなる組を作成し、前記第一周目の計算手段が再暗号に使用する為の公開鍵を作成する再暗号用公開鍵作成手段と、送られてきたデータを変換するデータ変換手段と、秘密鍵変換手段と、乱数変換手段とからなり、

前記データ変換手段が、前記データ本体である暗号文の組を、真理値群環上の多重配列エルガマル暗号文達と真理値群環上の拡張多重配列エルガマル暗号文達とからなる別の組に変換する為の手段であり、

前記秘密鍵変換手段が、前記データ変換手段の計算結果である暗号文達の組に使用されている秘密鍵を再暗号用公開鍵作成手段で作成された公開鍵に対応する秘密鍵に変換する手段であり、

前記秘密鍵変換手段の計算結果が真理値群環上の多重配列エルガマル暗号文達と真理値群環上の拡張多重配列エルガマル暗号文達とからなる組であり、

前記乱数変換手段が前記データ変換手段の計算結果である暗号文達の組に使用されている乱数を変換する手段であり、

前記乱数変換手段の計算結果が真理値群環上の多重配列エルガマル暗号文達と真理値群環上の拡張多重配列エルガマル暗号文達とからなる組である事を特徴とする計算システム。

９．　請求項８に記載されている計算システムにおいて、

第一周目以降の周の計算手段が、第二周目の計算手段と第二周目以降の計算手段とからなり、

前記送られてきたデータのデータ本体と前記本計算で計算されたデータ本体とが、第二周目の計算では、共に真理値群環上の多重配列エルガマル暗号文達と真理値群環上の拡張多重配列エルガマル暗号文達とからなる組であり、

前記第二周目の計算手段が、

前記送られてきたデータの前記データ本体を変換してエルガマル暗号文もしくは楕円曲線エルガマル暗号文を作成する暗号変換手段と、前記送られてきたデータのデータ本体の暗号文達を部分復号する部分復号手段とからなる計算システム。

１０．　請求項９に記載されている計算システムにおいて、

第二周目以降の計算手段が、第三周目の計算手段のみからなり、第三周目の計算手段の前記本計算手段が、前記送られてきたデータをそのまま出力し、

前記正当性証明作成手段が空列を出力する計算システム。

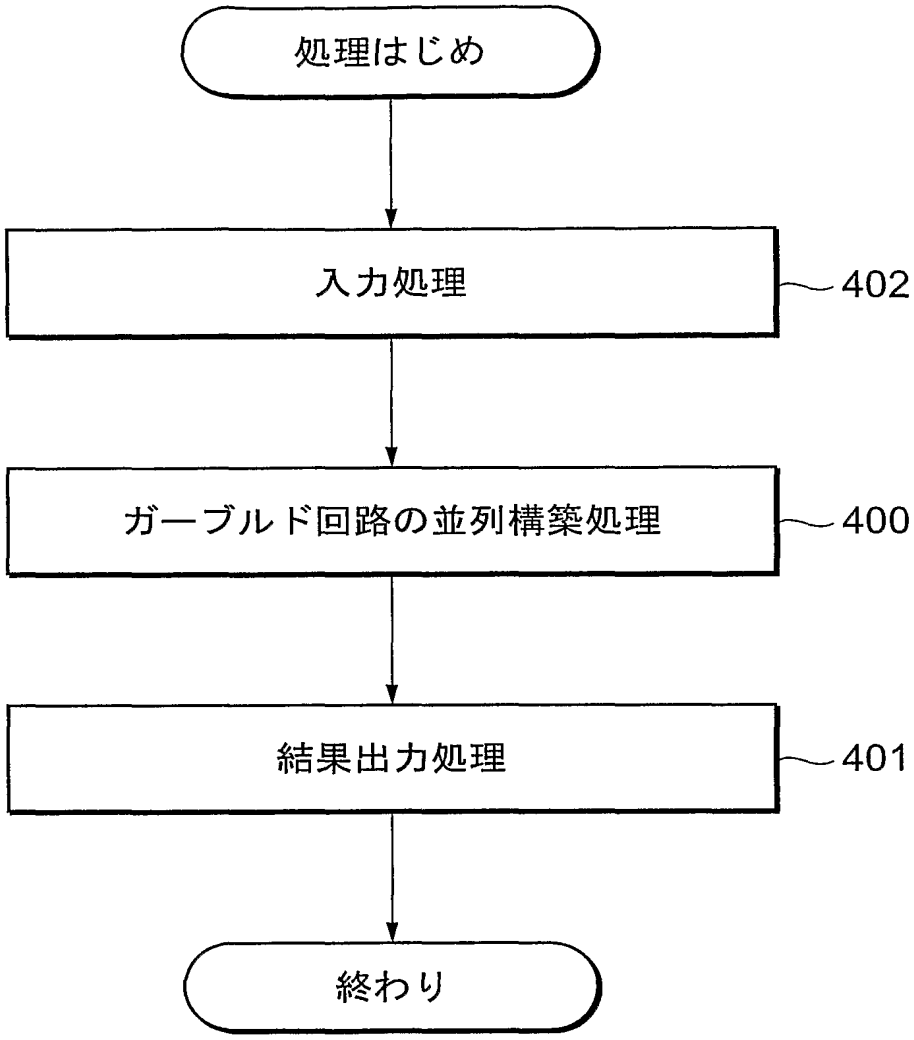


図1

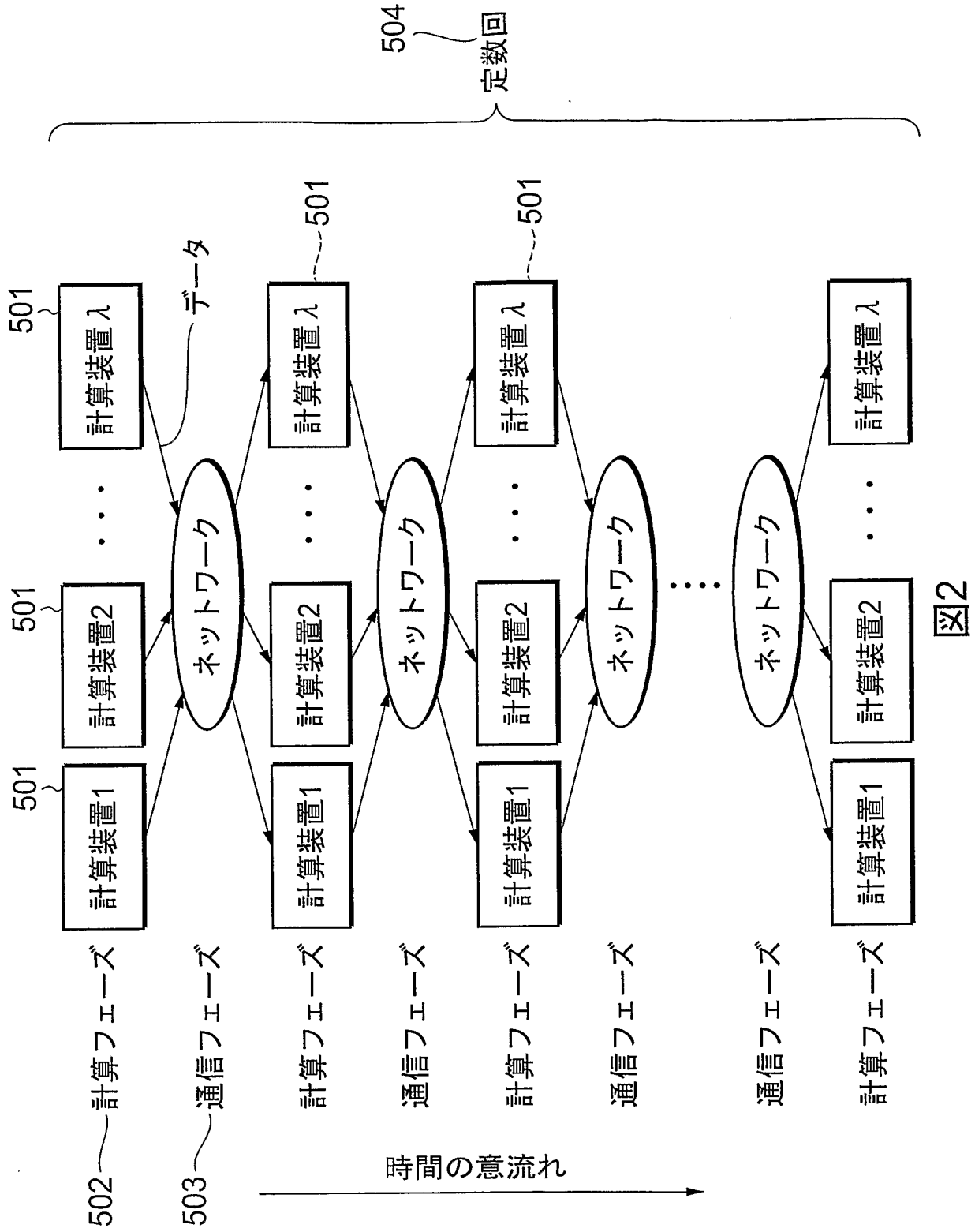

504
定数回
501
計算装置λ
データ
501
計算装置2
501
計算装置1
ネットワーク
計算装置λ
計算装置2
計算装置1
ネットワーク
計算装置λ
計算装置2
計算装置1
ネットワーク
計算装置λ
計算装置2
計算装置1
ネットワーク
502
計算フェーズ
503
通信フェーズ
計算フェーズ
通信フェーズ
計算フェーズ
通信フェーズ
通信フェーズ
計算フェーズ
時間の意流れ

図2

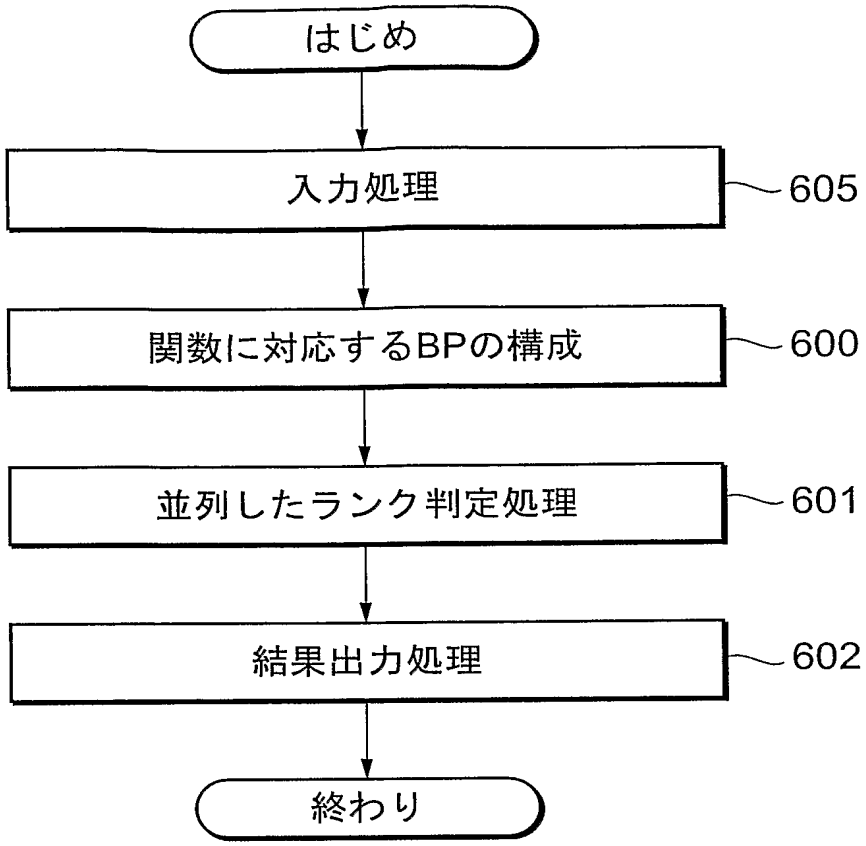

はじめ
入力処理
605
関数に対応するBPの構成
600
並列したランク判定処理
601
結果出力処理
602
終わり

図3

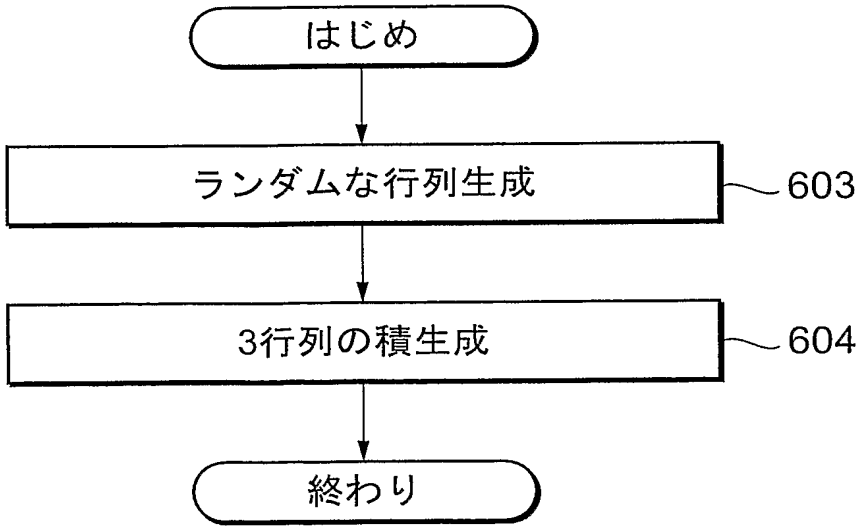

はじめ
ランダムな行列生成
603
3行列の積生成
604
終わり

図4

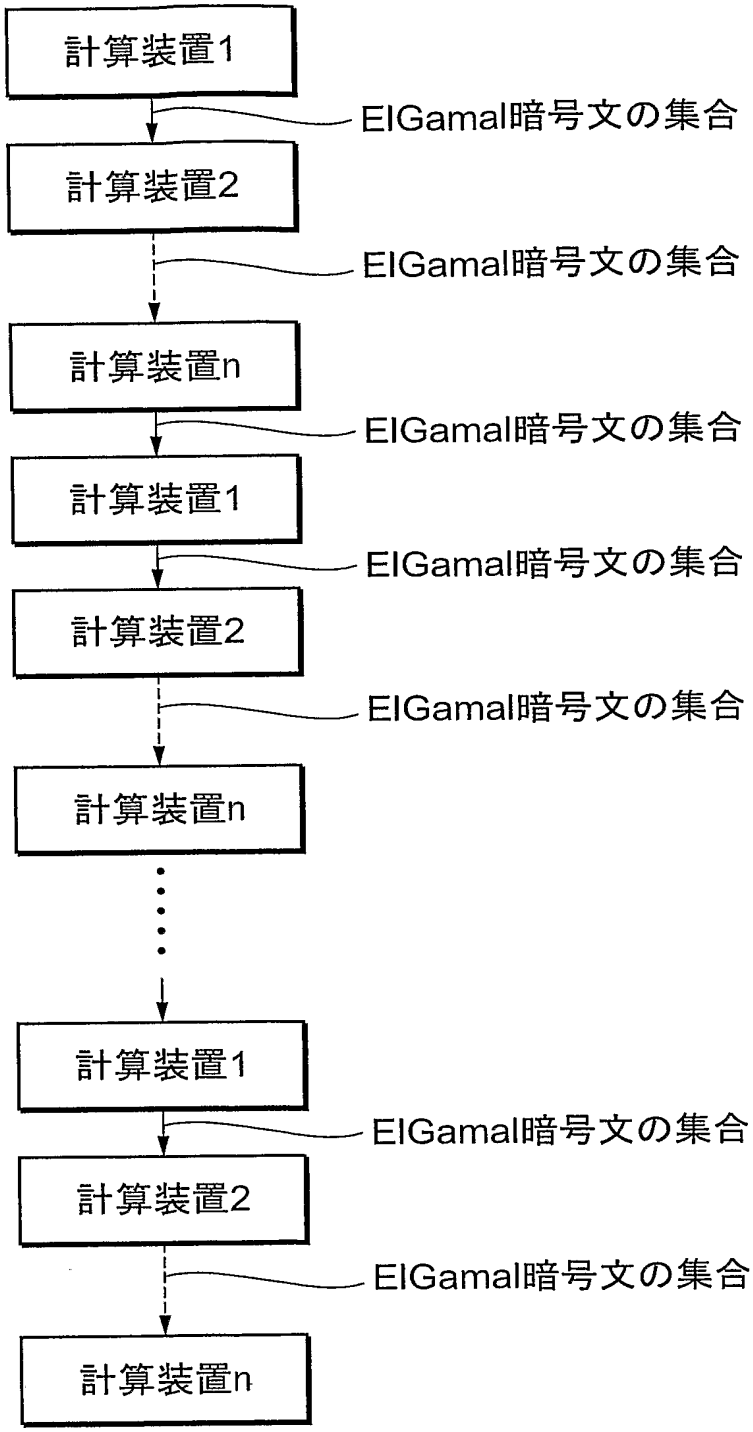

計算装置1
ElGamal暗号文の集合
計算装置2
ElGamal暗号文の集合
計算装置n
ElGamal暗号文の集合
計算装置1
ElGamal暗号文の集合
計算装置2
ElGamal暗号文の集合
計算装置n
計算装置1
ElGamal暗号文の集合
計算装置2
ElGamal暗号文の集合
計算装置n

図5

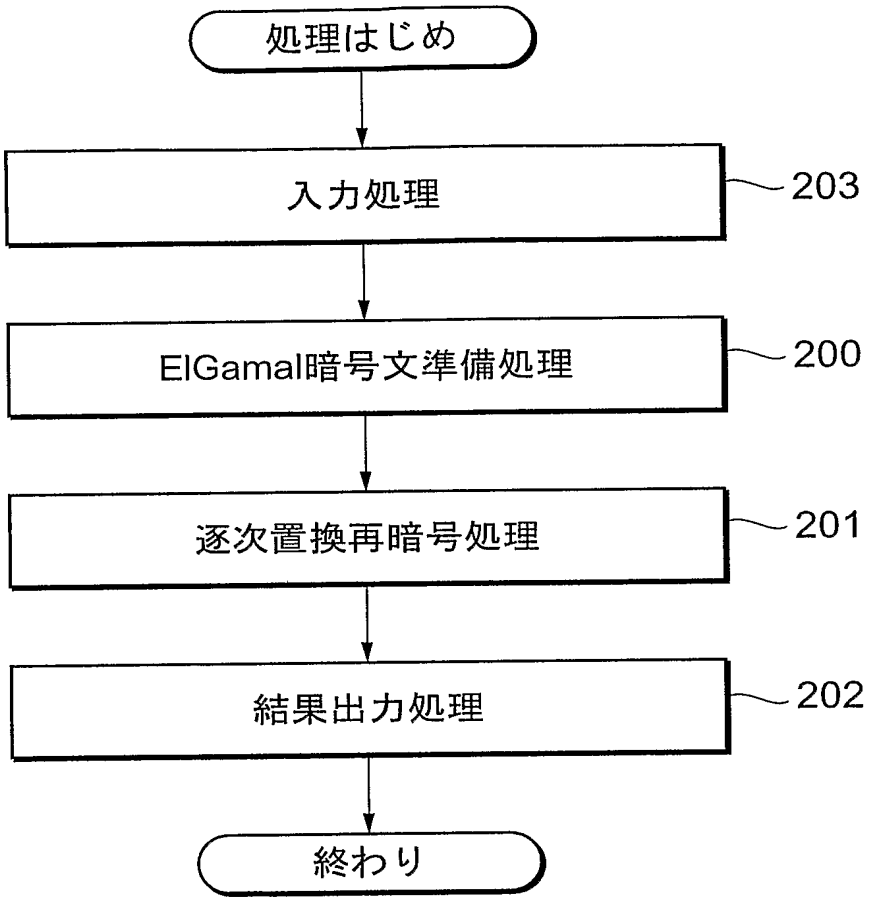

処理はじめ
入力処理
203
ElGamal暗号文準備処理
200
逐次置換再暗号処理
201
結果出力処理
202
終わり

図6

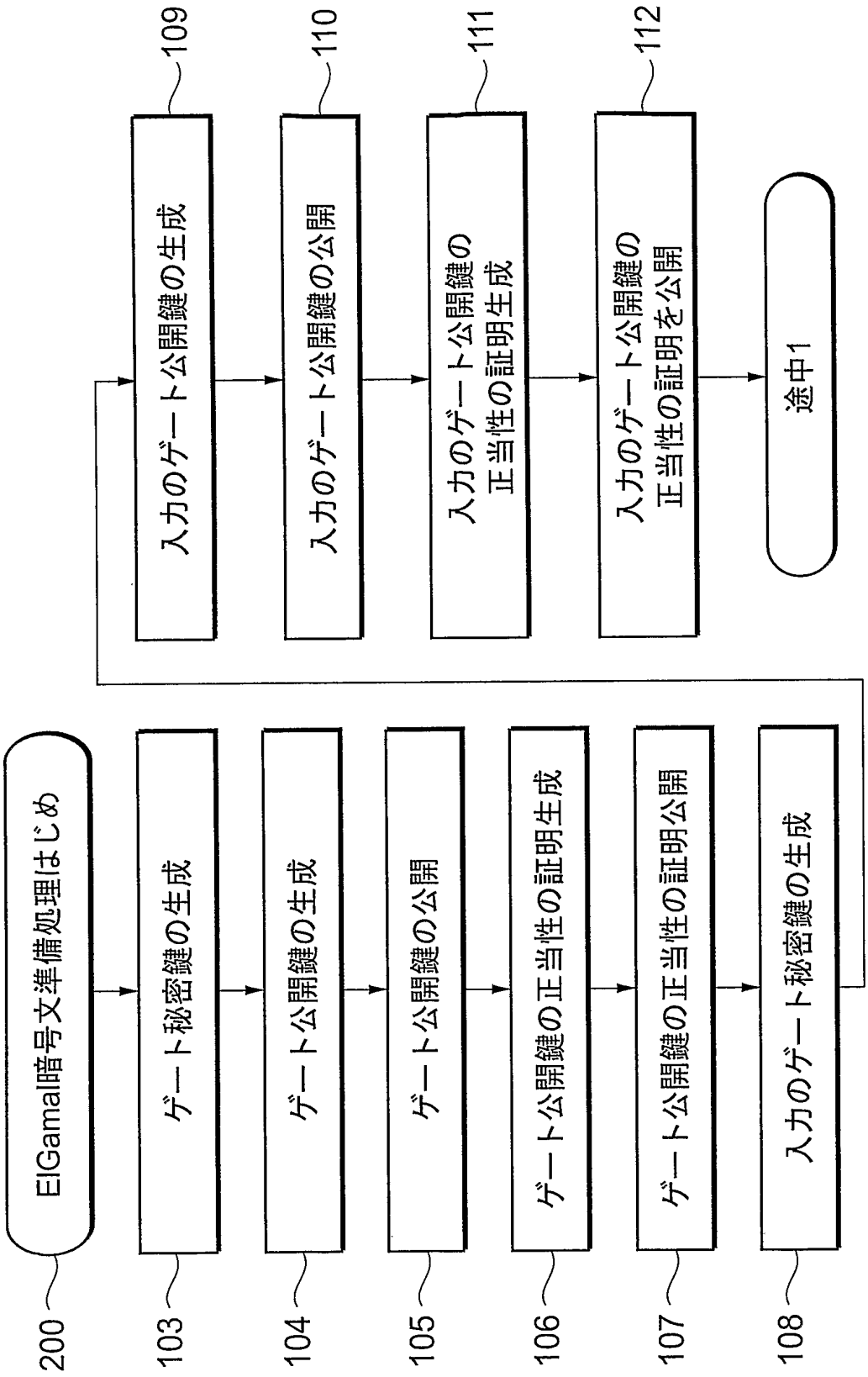

200
ElGamal暗号文準備処理はじめ
103
ゲート秘密鍵の生成
104
ゲート公開鍵の生成
105
ゲート公開鍵の公開
106
ゲート公開鍵の正当性の証明生成
107
ゲート公開鍵の正当性の証明公開
108
入力のゲート秘密鍵の生成
109
入力のゲート公開鍵の生成
110
入力のゲート公開鍵の公開
111
入力のゲート公開鍵の
正当性の証明生成
112
入力のゲート公開鍵の
正当性の証明を公開
途中1

図7

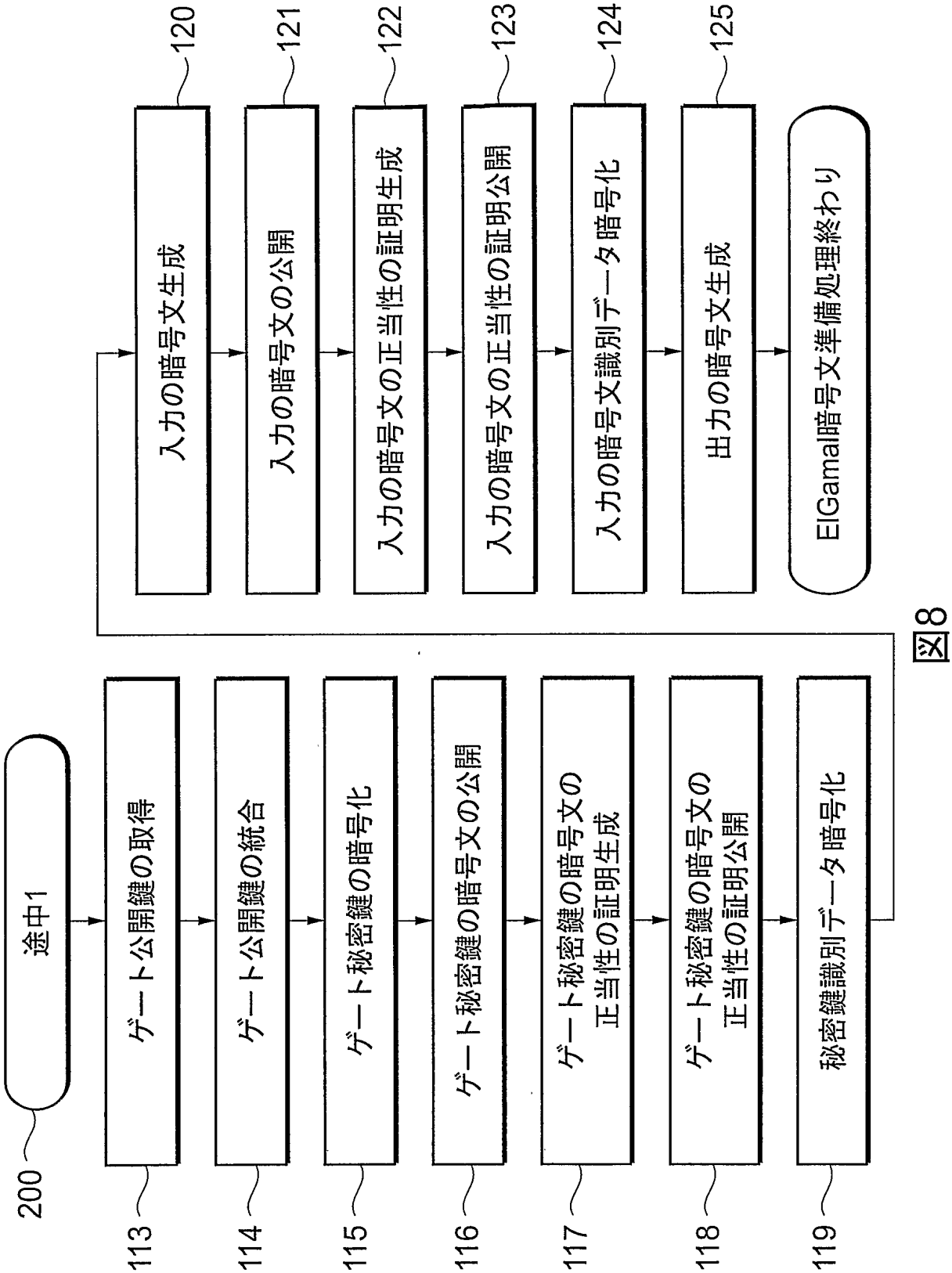

200
途中1
113
ゲート公開鍵の取得
114
ゲート公開鍵の統合
115
ゲート秘密鍵の暗号化
116
ゲート秘密鍵の暗号文の公開
117
ゲート秘密鍵の暗号文の正当性の証明生成
118
ゲート秘密鍵の暗号文の正当性の証明公開
119
秘密鍵識別データ暗号化
120
入力の暗号文生成
121
入力の暗号文の公開
122
入力の暗号文の正当性の証明生成
123
入力の暗号文の正当性の証明公開
124
入力の暗号文識別データ暗号化
125
出力の暗号文生成
ElGamal暗号文準備処理終わり

図8

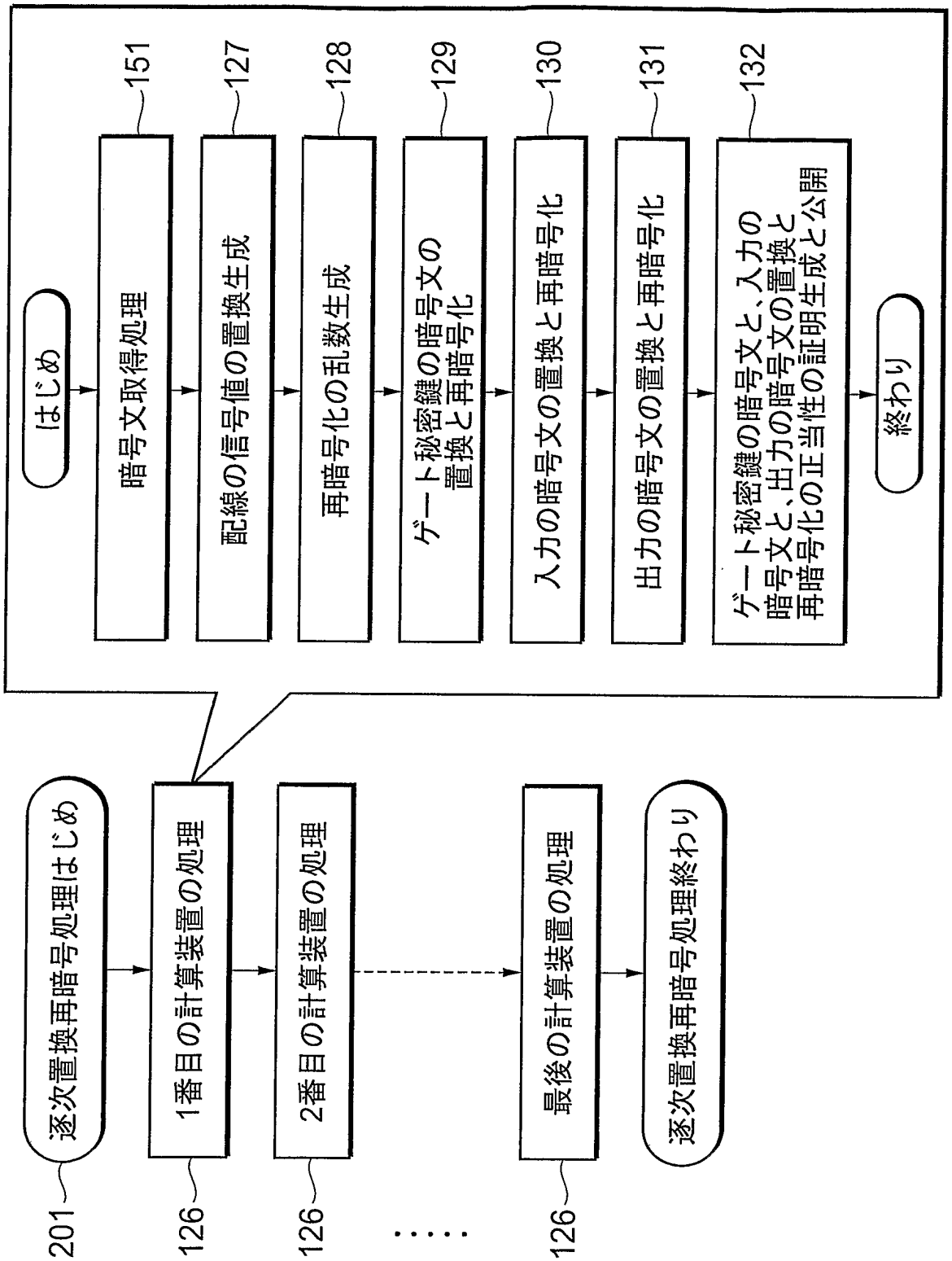

はじめ
暗号文取得処理
151
配線の信号値の置換生成
127
再暗号化の乱数生成
128
ゲート秘密鍵の暗号文の
置換と再暗号化
129
入力の暗号文の置換と再暗号化
130
出力の暗号文の置換と再暗号化
131
ゲート秘密鍵の暗号文と、入力の
暗号文と、出力の暗号文の置換と
再暗号化の正当性の証明生成と公開
132
終わり
逐次置換再暗号処理はじめ
201
1番目の計算装置の処理
126
2番目の計算装置の処理
126
・・・・
最後の計算装置の処理
126
逐次置換再暗号処理終わり

図9

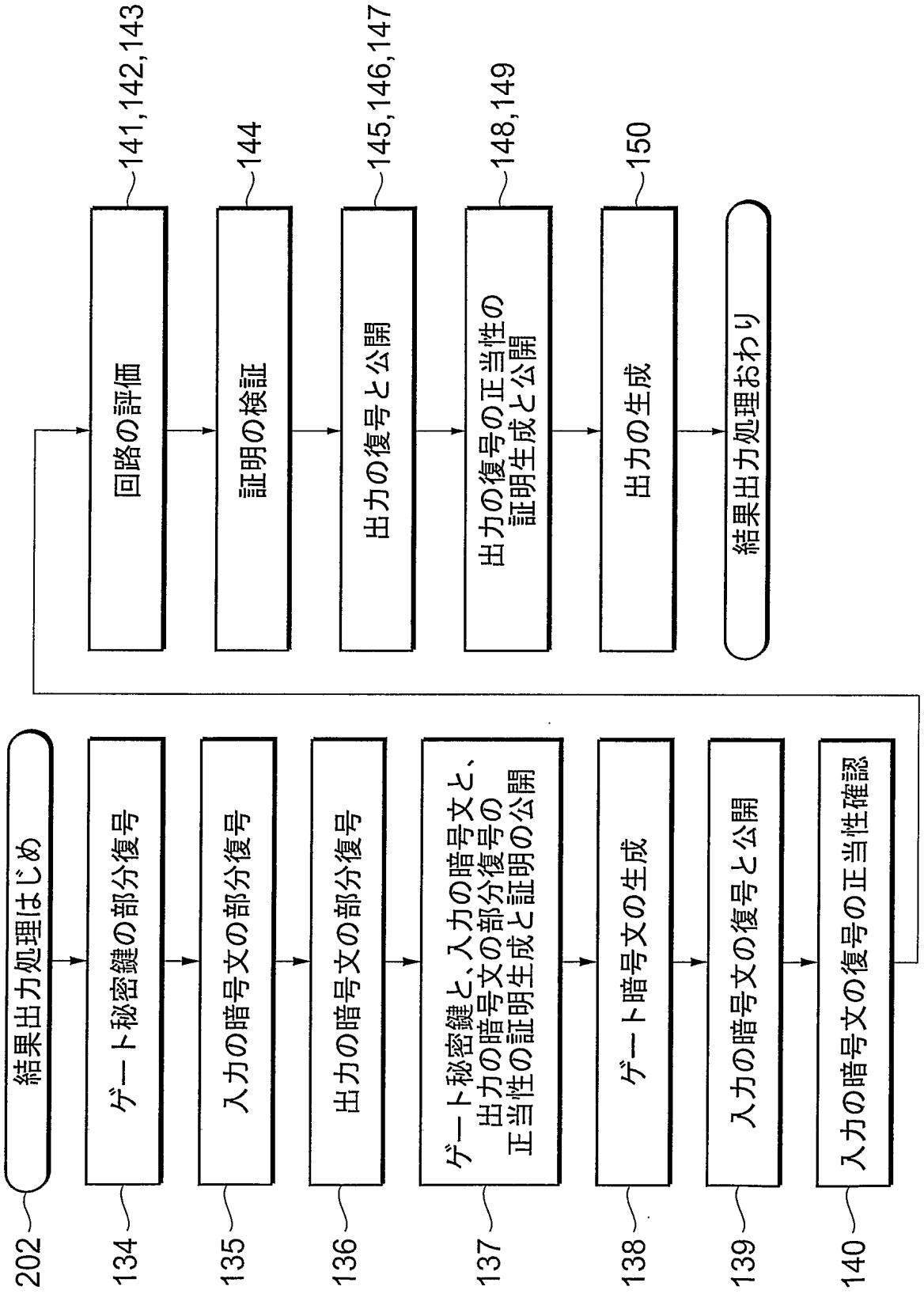

202
結果出力処理はじめ
134
ゲート秘密鍵の部分復号
135
入力の暗号文の部分復号
136
出力の暗号文の部分復号
137
ゲート秘密鍵と、入力の暗号文と、出力の暗号文の部分復号の正当性の証明生成と証明の公開
138
ゲート暗号文の生成
139
入力の暗号文の復号と公開
140
入力の暗号文の復号の正当性確認
141,142,143
回路の評価
144
証明の検証
145,146,147
出力の復号と公開
148,149
出力の復号の正当性の証明生成と公開
150
出力の生成
結果出力処理おわり

図10

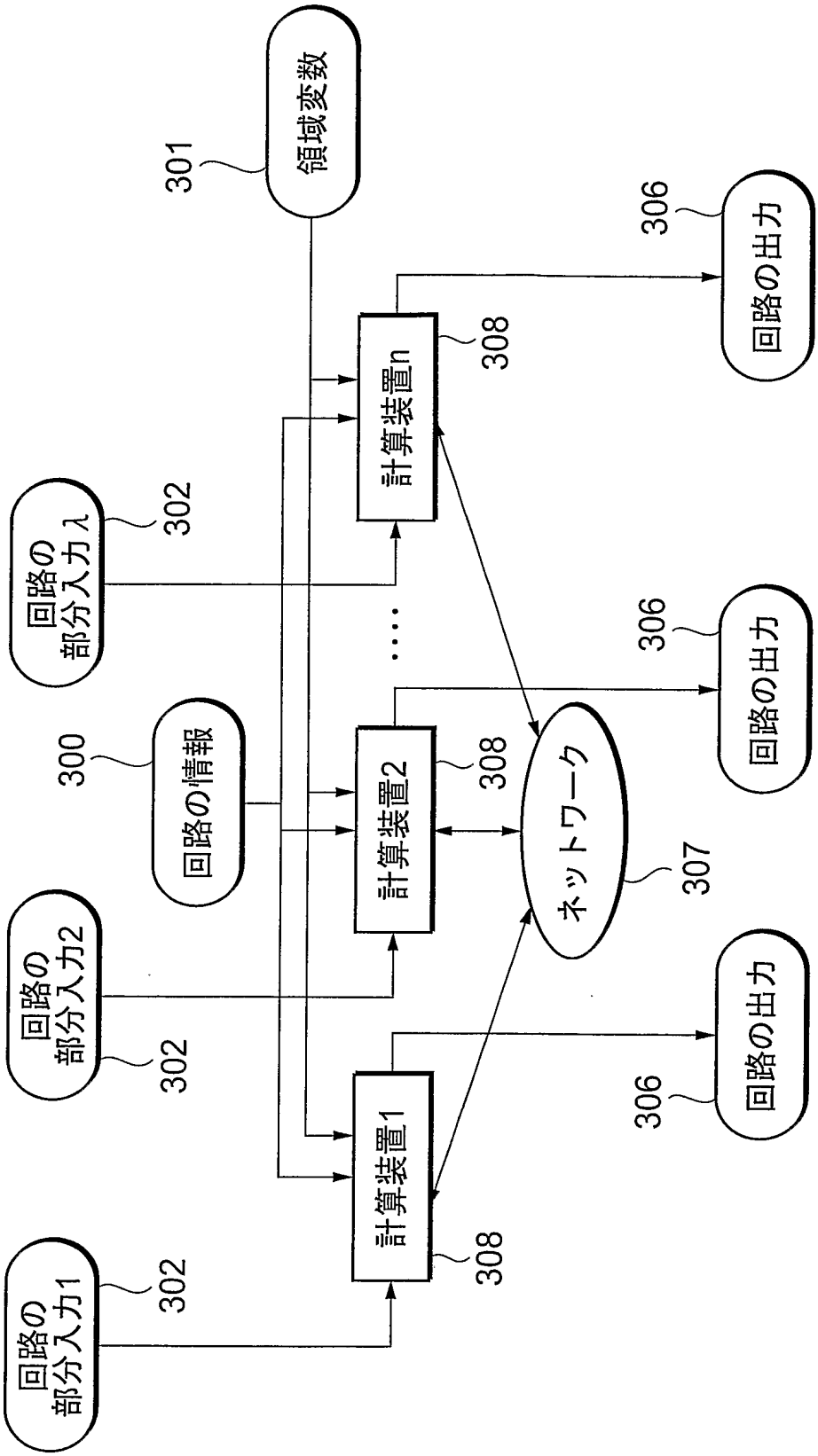

領域変数
301
回路の情報
300
回路の部分入力1
回路の部分入力2
回路の部分入力λ
302
計算装置1
計算装置2
計算装置n
308
ネットワーク
307
回路の出力
306

図11

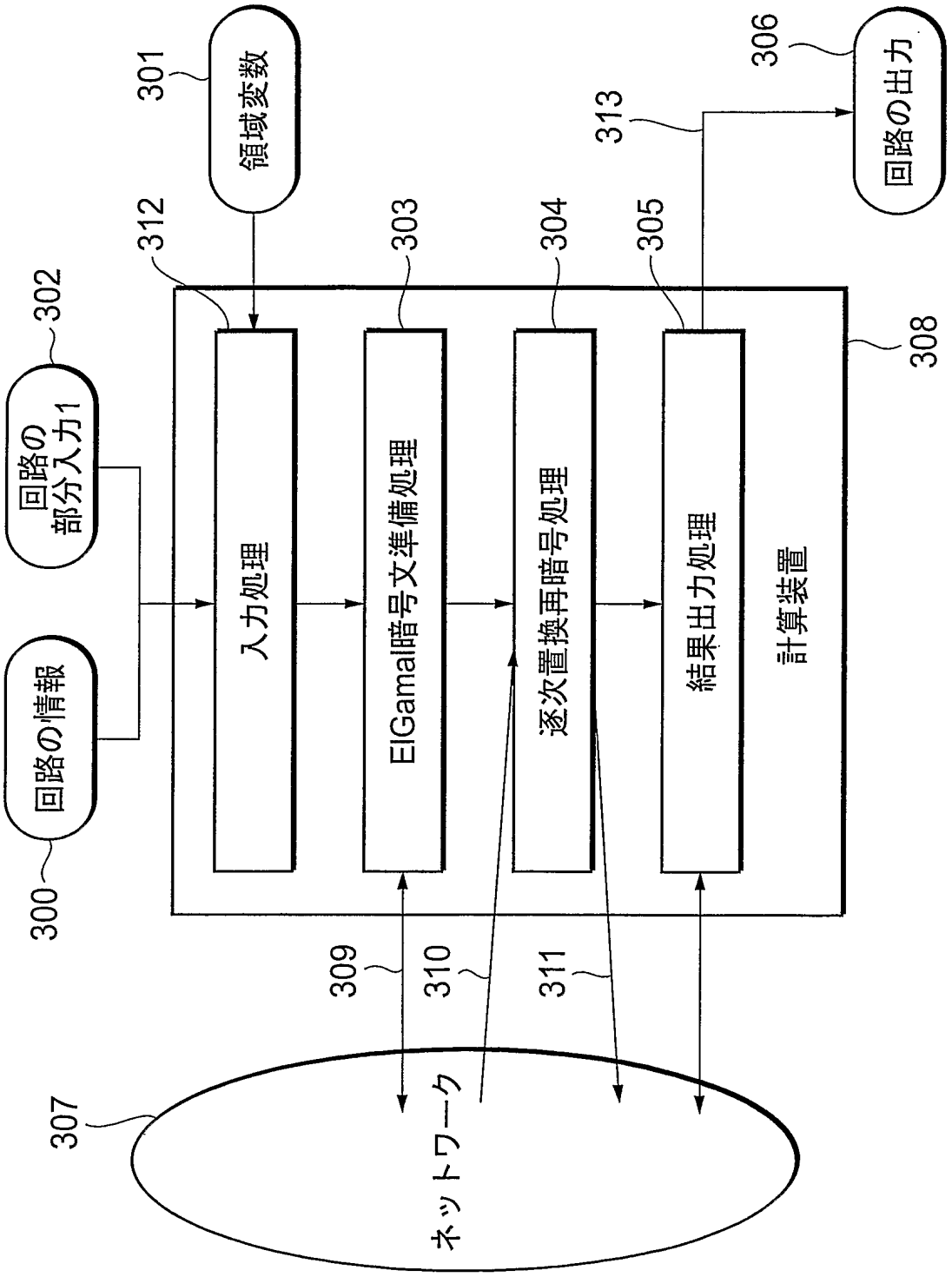

回路の情報
回路の部分入力1
領域変数
回路の出力
入力処理
ElGamal暗号文準備処理
逐次置換再暗号処理
結果出力処理
計算装置
ネットワーク
300
301
302
303
304
305
306
307
308
309
310
311
312
313

図12

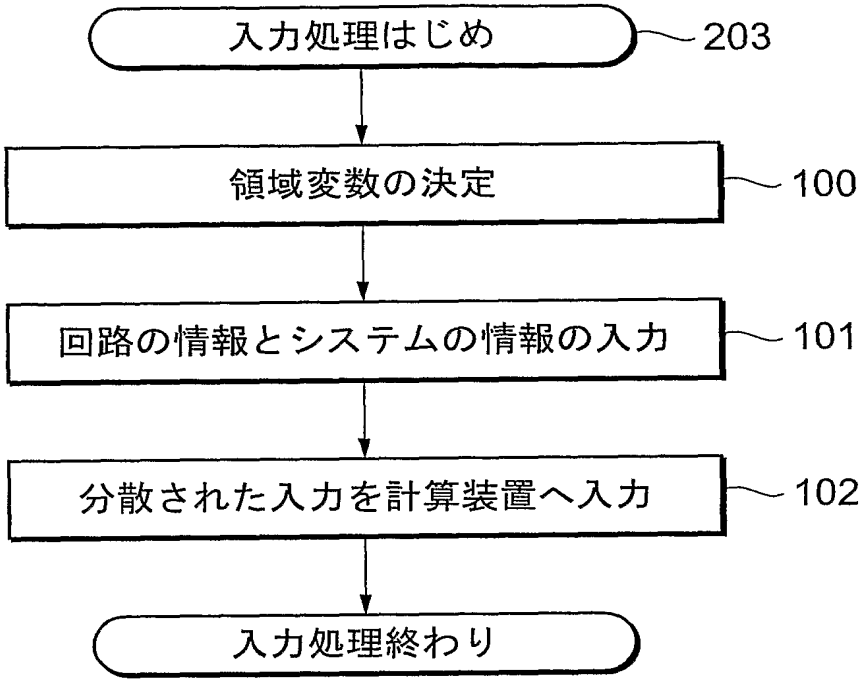

入力処理はじめ
203
領域変数の決定
100
回路の情報とシステムの情報の入力
101
分散された入力を計算装置へ入力
102
入力処理終わり

図13

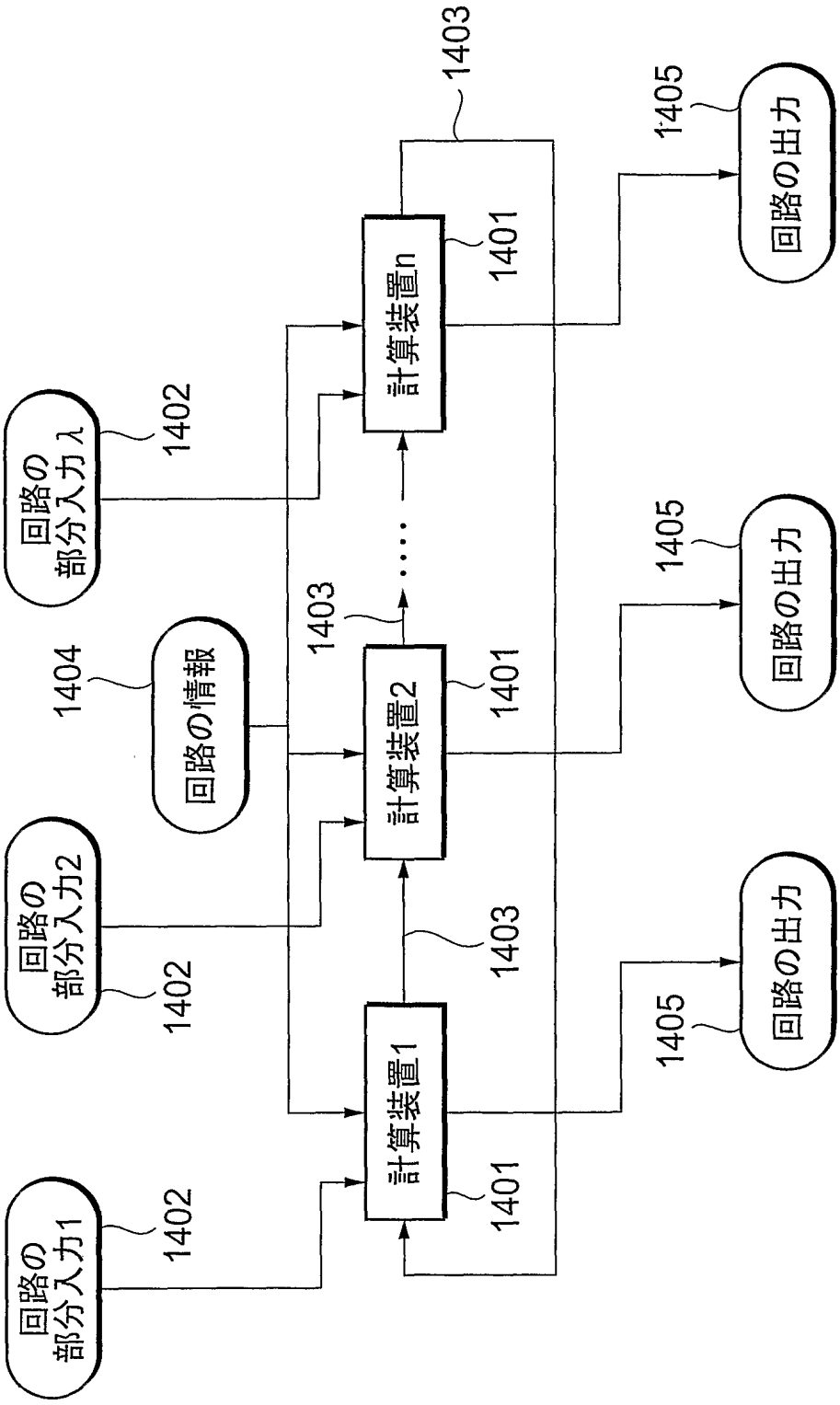

回路の
部分入力1
1402
回路の
部分入力2
1402
回路の
部分入力λ
1402
回路の情報
1404
計算装置1
1401
計算装置2
1401
計算装置n
1401
1403
1403
1403
1405
回路の出力
1405
回路の出力
1405
回路の出力

図14

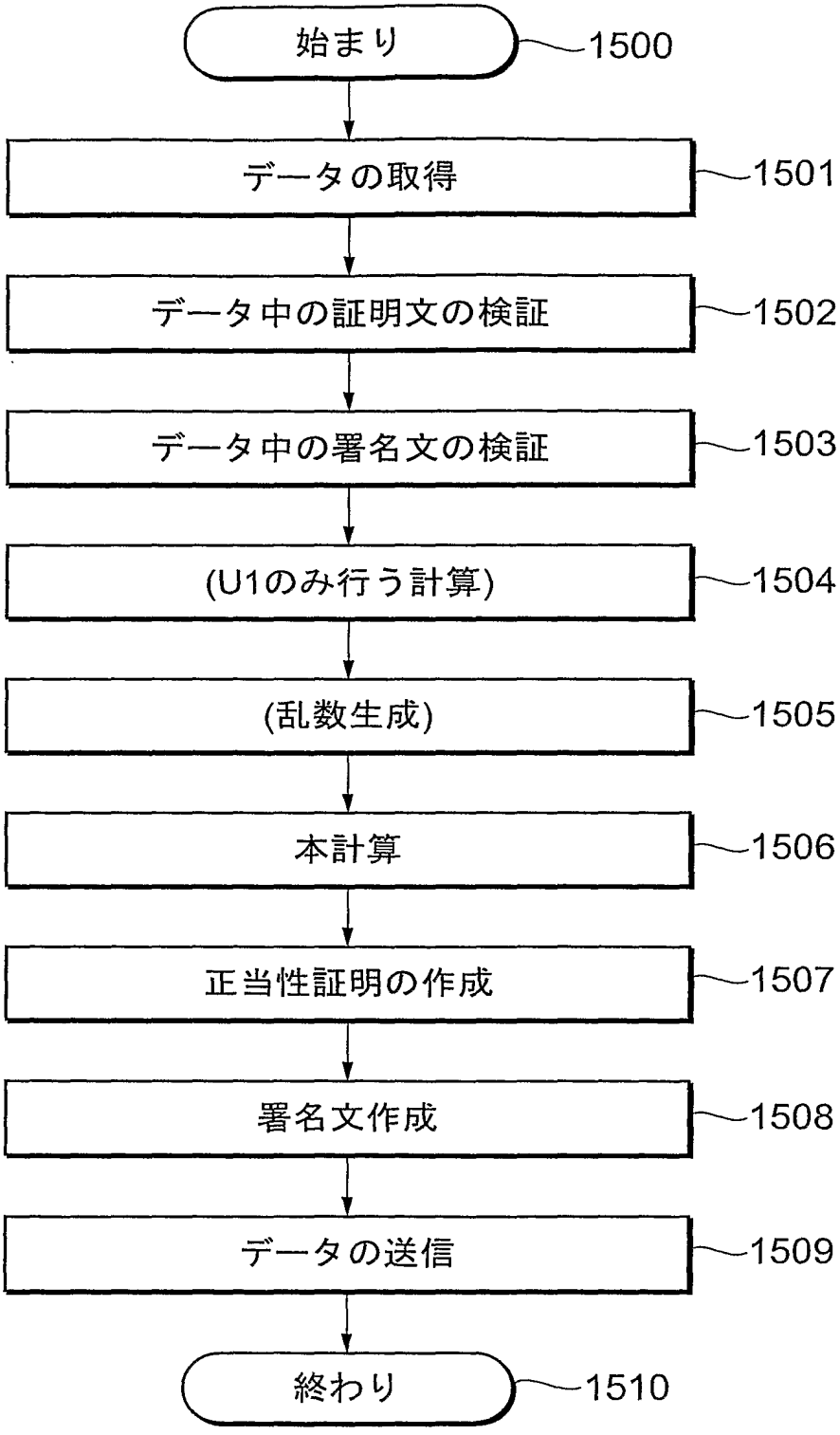

始まり
1500
データの取得
1501
データ中の証明文の検証
1502
データ中の署名文の検証
1503
(U1のみ行う計算)
1504
(乱数生成)
1505
本計算
1506
正当性証明の作成
1507
署名文作成
1508
データの送信
1509
終わり
1510

図15

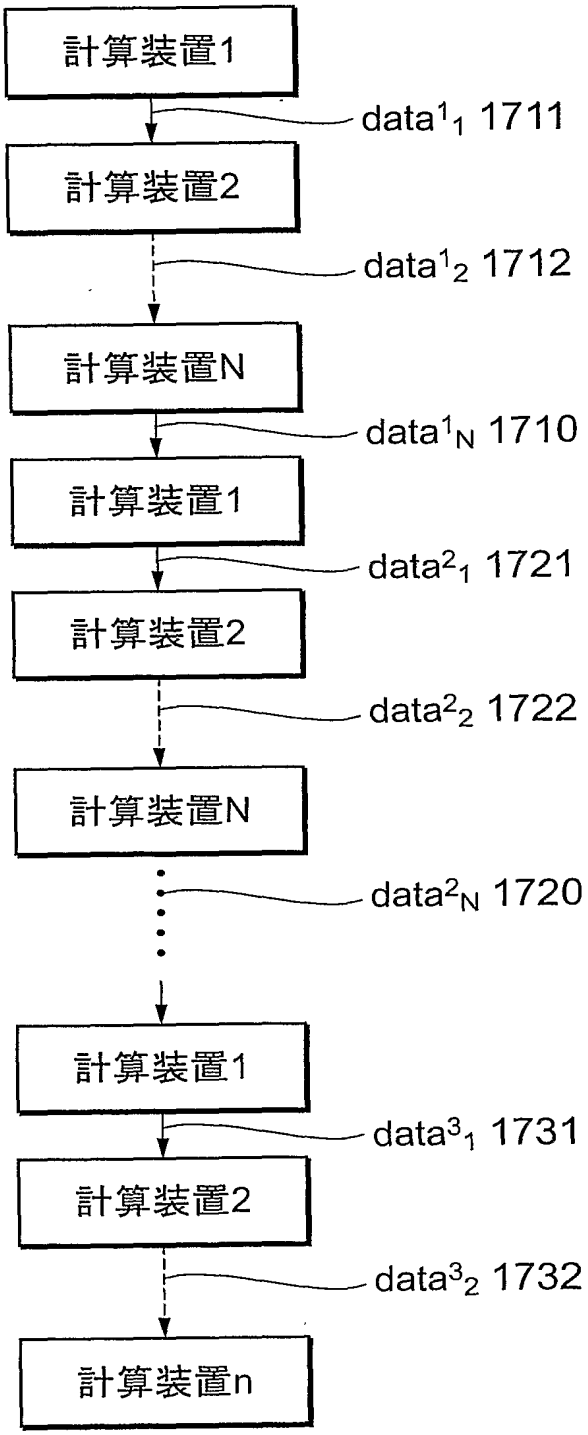

計算装置1
data$^1_1$ 1711
計算装置2
data$^1_2$ 1712
計算装置N
data^1_N 1710
計算装置1
data$^2_1$ 1721
計算装置2
data$^2_2$ 1722
計算装置N
data^2_N 1720
計算装置1
data$^3_1$ 1731
計算装置2
data$^3_2$ 1732
計算装置n

図16

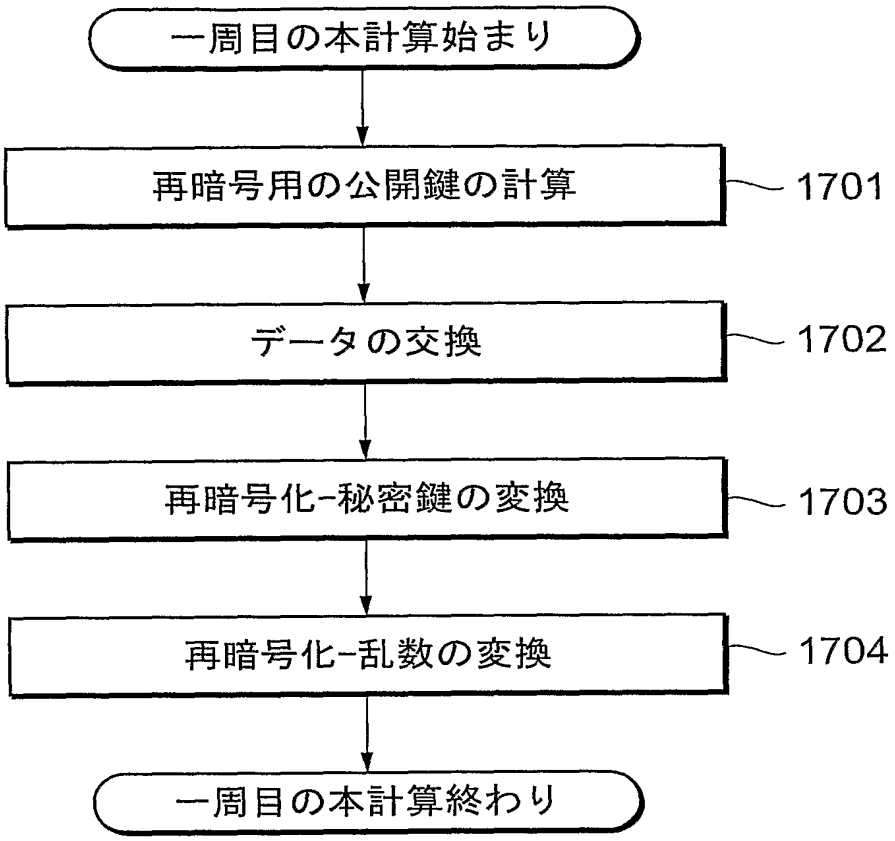

一周目の本計算始まり
再暗号用の公開鍵の計算
1701
データの交換
1702
再暗号化-秘密鍵の変換
1703
再暗号化-乱数の変換
1704
一周目の本計算終わり

図17

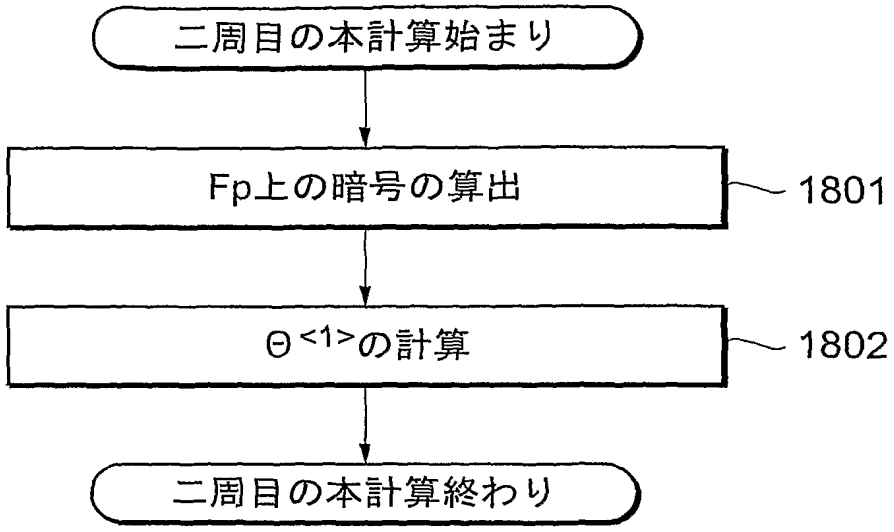

二周目の本計算始まり
Fp上の暗号の算出
1801
Θ<1>の計算
1802
二周目の本計算終わり

図18

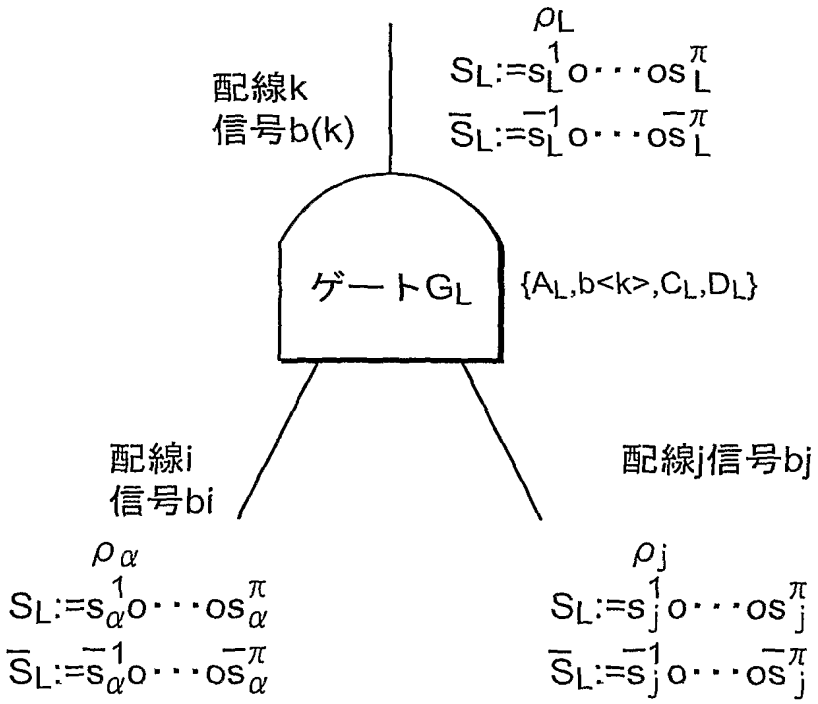

ρL
SL:=sL1o・・・osLπ
S̄L:=s̄L1o・・・os̄Lπ
配線k
信号b(k)
ゲートGL
{AL,b<k>,CL,DL}
配線i
信号bi
配線j信号bj
ρα
SL:=sα1o・・・osαπ
S̄L:=s̄α1o・・・os̄απ
ρj
SL:=sj1o・・・osjπ
S̄L:=s̄j1o・・・os̄jπ

図19

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/001437

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G09C1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Toroku Jitsuyo Shinan Koho 1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus FILE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2000-207483 A (Nippon Telegraph And Telephone Corp.), 28 July, 2000 (28.07.00), Par. Nos. [0041] to [0049]; Fig. 7 (Family: none)	1
Y A	JP 2002-237810 A (NEC Corp.), 23 August, 2002 (23.08.02), Par. Nos. [0001] to [0009]; Fig. 10 & US 2004/0114763 A1 & EP 1361693 A1 & WO 2002/065695 A1	2-4 5
Y A	D. Beaver, S. Micali, and P. Rogaway, "The round complexity of secure protocols", Annual ACM Symposium on Theory of Computing 22, 14 May, 1990 (14.05.90), pages 503 to 513	2-4 5-10

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 May, 2005 (24.05.05)	07 June, 2005 (07.06.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/001437

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Y. Ishai and E. Kushilevitz, "Randomizing Polynomials: A new Representation with Applications to Round-Efficient Secure Computation", IEEE Symposium on Foundations of Computer Science 2000, 22 January, 2001 (22.01.01), pages 294 to 304	6-10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/001437

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The matter common the inventions of claims 1-10 relates to a technique for calculating a given function by successively performing calculation by one computer after another which are linked to a device (hereinafter, referred to "technique X"). However, the search has revealed that the technique X is not novel since it is disclosed document JP 2000-207483 A (NEC Corp.), 28 July, 2000 (28.07.00), Par. No. [0041] to [0049], Fig. 7. As a result, the technique X makes no contribution over the prior art and the common matter (technique X) cannot be a special technical feature within the meaning of PCT Rule 13.2, second sentence.

(Continued to extra sheet)

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

Continuation of Box No.III of continuation of first sheet(2)

Accordingly, there exists no matter common to all the inventions of claims 1-10. The inventions of claims 1-10 are divided into three groups: the invention of claim 1, the inventions of claims 2-5, and the inventions of claims 6-10. Since between these groups of inventions, there exists no other common feature which can be considered as a special technical feature within the meaning of PCT Rule 13.2, second sentence, no technical relationship within the meaning of PCT Rule 13 between the different inventions can be seen. Consequently, it is obvious that the inventions of claims 1-10 do not satisfy the requirement of unity of invention.

国際調査報告

国際出願番号 PCT／JP2005／001437

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl.[7] G09C1/00

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl.[7] G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2005年
日本国実用新案登録公報	1996－2005年
日本国登録実用新案公報	1994－2005年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JSTPlusファイル

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 2000-207483 A（日本電信電話株式会社）2000.07.28, 段落【0041】－【0049】, 図7 （ファミリーなし）	1
Y A	JP 2002-237810 A（日本電気株式会社）2002.08.23, 段落【0001】－【0009】, 図10 & US 2004/0114763 A1 & EP 1361693 A1 & WO 2002/065695 A1	2-4 5
Y A	D. Beaver、S. Micali、and P. Rogaway, "The round complexity of secure protocols", Annual ACM Symposium on Theory of Computing	2-4 5-10

☑ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日 24.05.2005	国際調査報告の発送日 07.6.2005
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 5S 3574 中里 裕正 電話番号 03－3581－1101 内線 3546

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
	22, 1990.05.14, p.503-513	
A	Y. Ishai and E. Kushilevitz, "Randomizing Polynomials: A new Representation with Applications to Round-Efficient Secure Computation", IEEE Symposium on Foundations of Computer Science 2000, 2001.01.22, p.294-304	6-10

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００５／００１４３７

第Ⅱ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第8条第3項（ＰＣＴ17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

１．☐ 請求の範囲＿＿＿＿＿＿＿＿＿＿ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、

２．☐ 請求の範囲＿＿＿＿＿＿＿＿＿＿ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

３．☐ 請求の範囲＿＿＿＿＿＿＿＿＿＿ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第3文の規定に従って記載されていない。

第Ⅲ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲１－１０に係る発明の共通の事項は、機器を構成する複数の計算装置を連鎖させ、順に計算を行ってゆくことにより、与えられた関数の値を計算する技術（以下「技術Ｘ」という。）である。しかしながら、調査の結果、技術Ｘは、文献ＪＰ　２０００－２０７４８３　Ａ（日本電信電話株式会社）２０００．０７．２８，段落【００４１】－【００４９】，図７に開示されているから、新規でないことが明らかとなった。結果として、技術Ｘは先行技術の域を出ないから、ＰＣＴ規則１３．２の第２文の意味において、この共通事項（技術Ｘ）は特別な技術的特徴ではない。それ故、請求の範囲１－１０に係る発明全てに共通の事項はなく、請求の範囲１－１０は、請求の範囲１に係る発明、請求の範囲２－５に係る発明、及び、請求の範囲６－１０に係る発明の３群の発明に分けられるものと認められる。これら３群の発明は、ＰＣＴ規則１３．２の第２文の意味において特別な技術的特徴と考えられる他の共通の事項は存在しないので、それらの相違する発明の間にＰＣＴ規則１３の意味における技術的な関連を見いだすことはできない。よって、請求の範囲１－１０に係る発明は発明の単一性の要件を満たしていないことが明らかである。

１．☑ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

２．☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

３．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

４．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☑ 追加調査手数料の納付と共に出願人から異議申立てがなかった。